ПРИКАЗ ОПЕРАТИВНО-АНАЛИТИЧЕСКОГО ЦЕНТРА ПРИ ПРЕЗИДЕНТЕ РЕСПУБЛИКИ БЕЛАРУСЬ
20 февраля 2020 г. № 66

О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449

Изменения и дополнения:

Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 12 ноября 2021 г. № 195 (зарегистрировано в Национальном реестре - № 7/4893 от 15.11.2021 г.) <T62104893>;

Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 29 декабря 2022 г. № 210 (зарегистрировано в Национальном реестре - № 7/5249 от 29.12.2022 г.) <T62205249>;

Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 10 декабря 2024 г. № 259 (зарегистрировано в Национальном реестре - № 7/5889 от 12.12.2024 г.) <T62405889>

Во исполнение пункта 4 и абзаца третьего пункта 5 Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449 «О совершенствовании государственного регулирования в области защиты информации» ПРИКАЗЫВАЮ:

1. Утвердить:

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

Положение о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено (прилагается);

Положение о порядке технической и криптографической защиты информации, обрабатываемой на критически важных объектах информатизации (прилагается);

Положение о порядке представления в Оперативно-аналитический центр при Президенте Республики Беларусь сведений о событиях информационной безопасности, состоянии технической и криптографической защиты информации (прилагается);

Положение о порядке ведения Государственного реестра критически важных объектов информатизации (прилагается).

2. Определить:

форму заключения о соответствии объекта информатизации критериям отнесения объектов информатизации к критически важным и показателям уровня вероятного ущерба национальным интересам Республики Беларусь согласно приложению 1;

форму заключения об объединении критически важных объектов информатизации согласно приложению 2.

3. Внести изменения в следующие приказы Оперативно-аналитического центра при Президенте Республики Беларусь:

3.1. в приказе Оперативно-аналитического центра при Президенте Республики Беларусь от 29 июля 2013 г. № 48 «Об утверждении Инструкции о порядке осуществления контроля за технической защитой государственных секретов»:

преамбулу изложить в следующей редакции:

«На основании абзаца четвертого статьи 9 Закона Республики Беларусь от 19 июля 2010 г. № 170-З «О государственных секретах» ПРИКАЗЫВАЮ:»;

в пункте 1:

слово «прилагаемую» исключить;

дополнить пункт словом «(прилагается)»;

Инструкцию о порядке осуществления контроля за технической защитой государственных секретов, утвержденную этим приказом, изложить в новой редакции (прилагается);

3.2. в приказе Оперативно-аналитического центра при Президенте Республики Беларусь от 26 августа 2013 г. № 60 «Об утверждении Положения о порядке проведения государственной экспертизы средств технической и криптографической защиты информации»:

преамбулу изложить в следующей редакции:

«На основании абзаца третьего подпункта 6.6 пункта 6 Положения о технической и криптографической защите информации, утвержденного Указом Президента Республики Беларусь от 16 апреля 2013 г. № 196, ПРИКАЗЫВАЮ:»;

в пункте 1:

слово «прилагаемое» исключить;

дополнить пункт словом «(прилагается)»;

в Положении о порядке проведения государственной экспертизы средств технической и криптографической защиты информации, утвержденном этим приказом:

пункт 1 изложить в следующей редакции:

«1. В настоящем Положении определяется порядок проведения государственной экспертизы средств технической и криптографической защиты информации, за исключением средств шифрованной, других видов специальной связи и криптографических средств защиты государственных секретов.»;

в пункте 2:

абзац первый изложить в следующей редакции:

«2. Для целей настоящего Положения применяются термины в значениях, определенных в Положении о технической и криптографической защите информации, а также следующие термины и их определения:»;

из абзаца второго слова «(далее – ТНПА)» исключить;

абзац четвертый исключить;

из пункта 11 слова «к настоящему Положению» исключить;

из части второй пункта 12 слова «и печатью» исключить;

абзац второй пункта 14 исключить;

в абзаце четвертом пункта 17 и абзаце третьем части второй пункта 19 слово «местонахождение» заменить словами «место нахождения»;

из части первой пункта 20 слова «к настоящему Положению» исключить;

в части второй пункта 34:

слова «, иностранной организации» исключить;

после слова «отчество» дополнить часть словами «(если таковое имеется) и место жительства»;

приложения 1 и 2 к этому Положению изложить в новой редакции (прилагаются);

3.3. в Инструкции о порядке проведения аккредитации поставщиков услуг в Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь и осуществления контроля за соблюдением условий аккредитации, утвержденной приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 29 ноября 2013 г. № 89:

из пункта 2 слова «, техническими нормативными правовыми актами в сфере защиты информации» исключить;

приложения 1 и 3 к этой Инструкции изложить в новой редакции (прилагаются);

3.4. в Положении о Государственной системе управления открытыми ключами проверки электронной цифровой подписи Республики Беларусь, утвержденном приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 10 декабря 2015 г. № 118:

из абзаца первого пункта 2 слова «в Республике Беларусь» и «техническими нормативными правовыми актами,» исключить;

в части второй пункта 6 слова «НЦЭУ и утвержденной» заменить словами «и утвержденной НЦЭУ по согласованию с».

4. Исключен.

5. Действие абзацев второго и третьего пункта 1 настоящего приказа не распространяется на:

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

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

По истечении срока действия аттестата соответствия собственники (владельцы) информационных систем, указанных в части первой настоящего пункта, проводят повторную аттестацию (обращаются за проведением повторной аттестации) систем защиты информации информационных систем в порядке, установленном настоящим приказом.

Собственники (владельцы) информационных систем, указанных в части первой настоящего пункта, вправе руководствоваться настоящим приказом без учета переходных положений, определенных частями первой и второй настоящего пункта.

6. Системы безопасности критически важных объектов информатизации, созданные до вступления в силу настоящего приказа, подлежат приведению в соответствие с требованиями настоящего приказа в шестимесячный срок со дня вступления его в силу.

7. Признать утратившими силу:

приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20 декабря 2011 г. № 96 «О некоторых мерах по реализации Указа Президента Республики Беларусь от 25 октября 2011 г. № 486»;

приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 30 апреля 2012 г. № 42 «Об утверждении Инструкции о порядке проведения внешнего контроля за обеспечением безопасности критически важных объектов информатизации»;

приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 29 июля 2013 г. № 49 «Об утверждении Положения о порядке предоставления в Оперативно-аналитический центр при Президенте Республики Беларусь сведений о состоянии технической защиты информации»;

подпункты 1.3 и 1.4 пункта 1 приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 30 июля 2013 г. № 51 «О некоторых мерах по реализации Указа Президента Республики Беларусь от 16 апреля 2013 г. № 196»;

приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 30 августа 2013 г. № 62 «О некоторых вопросах технической и криптографической защиты информации»;

приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 16 января 2015 г. № 3 «О внесении дополнений и изменений в приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 30 августа 2013 г. № 62»;

приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 26 августа 2015 г. № 77 «О внесении изменений и дополнений в приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 29 июля 2013 г. № 49»;

подпункты 1.1 и 1.2 пункта 1 и пункт 2 приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 11 октября 2017 г. № 64 «О внесении изменений в некоторые приказы Оперативно-аналитического центра при Президенте Республики Беларусь»;

приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 12 октября 2018 г. № 151 «Об утверждении Положения об обеспечении безопасности критически важных объектов информатизации».

8. Настоящий приказ вступает в силу с 14 марта 2020 г.

Начальник **А.Ю.Павлюченко**

Приложение 1
к приказу
Оперативно-аналитического
центра при Президенте
Республики Беларусь
20.02.2020 № 66

Форма

УТВЕРЖДАЮ
_____
(наименование должности
_____
руководителя организации)
_____
(подпись, инициалы, фамилия)
__.__.20___

ЗАКЛЮЧЕНИЕ
о соответствии объекта информатизации критериям отнесения объектов информатизации к критически важным и показателям уровня вероятного ущерба национальным интересам Республики Беларусь

Комиссия _____
(полное наименование владельца объекта информатизации)
в составе:
председателя _____,
членов комиссии: _____
установила, что объект информатизации _____
(полное наименование
_____
объекта информатизации)
удовлетворяет условиям отнесения к критически важным объектам информатизации на основании его соответствия критерию (критериям) _____
(наименование критерия (критериев)
_____
отнесения объекта информатизации к критически важным объектам информатизации)
с показателем (показателями) уровня вероятного ущерба национальным интересам
_____
(показатель (показатели) уровня вероятного ущерба
_____
национальным интересам Республики Беларусь)

Председатель комиссии _____ _____
(подпись) (инициалы, фамилия)

Члены комиссии: _____ _____
(подпись) (инициалы, фамилия)

_____ _____
(подпись) (инициалы, фамилия)

Приложение 2
к приказу
Оперативно-аналитического
центра при Президенте
Республики Беларусь
20.02.2020 № 66

Форма

УТВЕРЖДАЮ

_____
(наименование должности

_____
руководителя организации)

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

ЗАКЛЮЧЕНИЕ
об объединении критически важных объектов информатизации

Комиссия _____
(полное наименование владельца критически важных объектов информатизации)
в составе:
председателя _____
членов комиссии: _____
установила, что критически важные объекты информатизации _____
(полное наименование
_____ в связи с
критически важных объектов информатизации)
_____
(указываются конкретные причины правового, организационного или технического характера,
_____
послужившие основанием для объединения критически важных объектов информатизации)
подлежат объединению в один критически важный объект информатизации
_____
(полное наименование
_____
критически важного объекта информатизации)

Председатель комиссии _____ _____
(подпись) (инициалы, фамилия)

Члены комиссии: _____ _____
(подпись) (инициалы, фамилия)

_____ _____
(подпись) (инициалы, фамилия)

УТВЕРЖДЕНО

Приказ
Оперативно-аналитического центра
при Президенте Республики Беларусь
20.02.2020 № 66
(в редакции приказа
Оперативно-аналитического центра
при Президенте Республики Беларусь
10.12.2024 № 259)

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

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

1. В настоящем Положении в соответствии с абзацем вторым подпункта 6.4 пункта 6 Положения о технической и криптографической защите информации, утвержденного Указом Президента Республики Беларусь от 16 апреля 2013 г. № 196, определяется порядок технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам.

Настоящее Положение может не применяться:

собственниками (владельцами) информационных систем, в которых обрабатываются только общедоступные персональные данные и (или) персональные данные, полученные после применения методов обезличивания, – в отношении таких информационных систем;

операторами электросвязи – собственниками (владельцами) информационных систем, обеспечивающих управление технологическими процессами и предназначенных только для передачи персональных данных по технологическим сетям электросвязи, – в отношении таких информационных систем. Для целей применения настоящего абзаца операторы электросвязи согласовывают с Оперативно-аналитическим центром при Президенте Республики Беларусь (далее – ОАЦ) перечни указанных информационных систем, к которым должны прилагаться структурная и логическая схемы каждой информационной системы, включенной в перечень.

2. Для целей настоящего Положения термины используются в значениях, определенных в Положении о технической и криптографической защите информации, Законе Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации», Законе Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных», а также следующие термины и их определения:

активы информационной системы – средства вычислительной техники, телекоммуникационное оборудование, системное и прикладное программное обеспечение, информационные ресурсы, входящие в состав информационной системы;

защищенный канал передачи данных – установленный между средствами криптографической защиты информации отправителя и получателя информации канал передачи данных, в котором конфиденциальность и контроль целостности передаваемой информации обеспечиваются криптографическими методами защиты информации;

компрометация криптографического ключа – событие, в результате которого криптографический ключ или его часть становятся известными лицам, не имеющим прав доступа к данному ключу.

3. Работы по технической и криптографической защите информации включают:

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, утвержденным приказом, утверждающим настоящее Положение;

обеспечение функционирования системы защиты информации в процессе эксплуатации информационной системы;

обеспечение защиты информации в случае прекращения эксплуатации информационной системы.

4. Работы по проектированию, созданию и (или) аттестации систем защиты информации у собственника (владельца) информационной системы могут выполняться:

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 среднее специальное, или профессионально-техническое образование и пройти переподготовку или повышение квалификации по вопросам технической и криптографической защиты информации в порядке, установленном законодательством;

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

Физические лица, являющиеся собственниками информационных систем, в которых обрабатываются персональные данные, вправе выполнять работы по проектированию и (или) созданию систем защиты информации этих информационных систем самостоятельно (без создания (назначения) подразделения защиты информации или иного подразделения (должностного лица), ответственного за обеспечение защиты информации) либо с привлечением специализированной организации.

5. Допускается применение единой системы защиты информации для нескольких информационных систем, принадлежащих одному собственнику (владельцу).

6. Перечень работ по технической и криптографической защите информации может предусматриваться в техническом задании на создание информационной системы.

7. При выполнении специализированными организациями работ по проектированию и (или) созданию систем защиты информации информационное взаимодействие между информационными системами должно осуществляться с использованием защищенных каналов передачи данных.

8. До проведения работ по проектированию системы защиты информации собственник (владелец) информационной системы в соответствии с законодательством об информации, информатизации и защите информации определяет вид информации, которая будет обрабатываться в информационной системе, и осуществляет отнесение информационной системы к классу (классам) типовых информационных систем согласно приложению 1.

Об отнесении информационной системы к классу (классам) типовых информационных систем составляется акт по форме согласно приложению 2. Физические лица, являющиеся собственниками информационных систем, в которых обрабатываются персональные данные, составляют акт отнесения информационной системы к классу (классам) типовых информационных систем в произвольной форме.

▶ГЛАВА 2
ПРОЕКТИРОВАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

9. На этапе проектирования системы защиты информации осуществляются:

разработка (корректировка) политики информационной безопасности. При этом физические лица, являющиеся собственниками информационных систем, в которых обрабатываются персональные данные, за исключением индивидуальных предпринимателей

и физических лиц, осуществляющих деятельность по оказанию услуг в сфере агроэкотуризма, вправе не разрабатывать политику информационной безопасности;

разработка структурной и логической схем информационной системы;

разработка технического задания на создание системы защиты информации (далее – техническое задание);

разработка проектов локальных правовых актов и других организационно-распорядительных документов по вопросам применения системы защиты информации.

На этапе проектирования системы защиты информации документы, указанные в абзацах втором–четвертом части первой настоящего пункта, утверждаются собственником (владельцем) информационной системы.

10. Политика информационной безопасности:

должна содержать цели и принципы защиты информации, обязательства собственника (владельца) информационной системы соответствовать требованиям по защите информации, постоянно совершенствовать систему защиты информации;

по решению собственника (владельца) информационной системы может содержать иную информацию, отражающую общие намерения по обеспечению конфиденциальности, целостности, подлинности, доступности и сохранности информации, обрабатываемой в информационной системе;

должна быть доведена до сведения работников собственника (владельца) информационной системы в части, их касающейся, быть доступной всем заинтересованным субъектам информационных отношений для ознакомления.

При наличии у одного собственника (владельца) нескольких информационных систем разрабатывается и утверждается единая политика информационной безопасности.

11. Структурная и логическая схемы информационной системы разрабатываются на основе анализа структуры информационной системы и информационных потоков (внутренних и внешних), состава, количества и мест размещения активов информационной системы, ее физических и логических границ.

Структурная схема информационной системы отражает особенности функционирования информационной системы на физическом и канальном уровнях и должна содержать:

наименование информационной системы;

места размещения физических устройств, относящихся к активам информационной системы, средств защиты информации с указанием названия устройства согласно его системному имени (серийный номер – для неуправляемого устройства), названий физических интерфейсов устройства;

физические линии связи с указанием их типа (витая пара, волоконно-оптический кабель и др.), идентификаторы виртуальных локальных вычислительных сетей (VLAN ID);

физические границы информационной системы.

К структурной схеме информационной системы должны прилагаться:

сведения о назначении линий связи (передача данных или управление активами информационной системы, средствами защиты информации);

перечень виртуальных локальных вычислительных сетей (VLAN) с указанием их идентификаторов (VLAN ID), названий виртуальных локальных вычислительных сетей (VLAN Name), IP-адресации, используемой в виртуальных локальных вычислительных сетях (VLAN);

перечень телекоммуникационного оборудования с указанием производителя оборудования, его модели, системного имени (серийного номера для неуправляемого устройства), IP-адреса управления устройством, места размещения (помещение, номер стойки, место в стойке и др.).

Логическая схема информационной системы отражает особенности функционирования информационной системы на сетевом и последующих уровнях и должна содержать:

наименование информационной системы;

направления информационных потоков (внутренних и внешних). Для информационных систем классов «3-ин», «3-спец», «3-бг», «3-дсп» и «3-юл» допускается взаимодействие с любыми информационными системами;

логические границы информационной системы.

К логической схеме информационной системы должны прилагаться сведения:

об информационных ресурсах, входящих в состав информационной системы, с указанием IP-адресов и названий физических серверов, виртуальных машин, контейнеров, обеспечивающих их функционирование;

о средствах защиты информации с указанием IP-адресов их администрирования;

об открытых портах транспортного уровня с указанием соответствующих им IP-адресов технологий и (или) протоколов.

Сведения, указанные в частях второй–пятой настоящего пункта, отражаются на структурной и логической схемах информационной системы и в приложениях к ним при наличии таких сведений.

В структурной и логической схемах информационной системы допускается объединение однотипных физических устройств, виртуальных машин, относящихся к активам информационной системы, средствам защиты информации, в единый элемент при условии наличия соответствующих обозначений, отражающих наполнение данного элемента.

Структурная и логическая схемы информационной системы и прилагаемые к ним документы составляются в произвольной форме с учетом особенностей функционирования информационной системы и должны обеспечивать читаемость содержащихся в них сведений.

12. Техническое задание разрабатывается собственником (владельцем) информационной системы либо специализированной организацией и утверждается собственником (владельцем) информационной системы.

Техническое задание должно содержать:

наименование информационной системы с указанием присвоенного (присвоенных) ей класса (классов) типовых информационных систем;

требования к системе защиты информации в зависимости от используемых технологий и класса типовых информационных систем на основе перечня согласно приложению 3;

порядок обезличивания персональных данных, если предполагается обезличивание персональных данных. Допустимые методы обезличивания определены согласно приложению 4;

требования из числа реализованных в аттестованной в установленном порядке системе защиты информации информационной системы другого собственника (владельца), если функционирование информационной системы, для которой осуществляется проектирование системы защиты информации, предполагается на базе информационной системы другого собственника (владельца) в соответствии с пунктом 15 настоящего Положения;

требования к средствам криптографической защиты информации на основе перечня государственных стандартов, взаимосвязанных с техническим регламентом Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY), утвержденным постановлением Совета Министров Республики Беларусь от 15 мая 2013 г. № 375.

Собственник (владелец) информационной системы вправе не включать в техническое задание отдельные обязательные требования к системе защиты информации по перечню согласно приложению 3 при отсутствии в информационной системе соответствующего актива (технологии) либо при условии согласования с ОАЦ закрепления в таком техническом задании обоснованных компенсирующих мер.

13. В локальных правовых актах и других организационно-распорядительных документах по вопросам применения системы защиты информации с учетом требований, определенных в техническом задании, должны быть регламентированы права и обязанности пользователей информационной системы, а также порядок применения системы защиты информации, в том числе порядок реализации мероприятий по:

выявлению угроз, которые могут привести к сбоям, нарушению функционирования информационной системы, реагированию на соответствующие события и ликвидации их последствий;

применению технологии электронной цифровой подписи (особенности выработки и проверки электронной цифровой подписи, обращения с личными ключами электронной цифровой подписи).

Формы документов, указанных в части первой настоящего пункта, определяются собственником (владельцем) информационной системы с учетом особенностей его деятельности.

Не допускается определение порядка применения системы защиты информации в локальных правовых актах организации по иным вопросам ее деятельности. При необходимости такие акты могут содержать отсылки к локальным правовым актам, указанным в части первой настоящего пункта.

Собственник (владелец) информационной системы обязан утвердить (в произвольной форме) и поддерживать в актуальном состоянии перечень локальных правовых актов и других организационно-распорядительных документов по вопросам применения системы защиты информации.

Локальные правовые акты и другие организационно-распорядительные документы по вопросам применения системы защиты информации должны быть доведены до сведения работников собственника (владельца) информационной системы в части, их касающейся.

14. При выборе мер по защите информации и регламентации порядка их реализации, а также при выборе компенсирующих мер собственник (владелец) информационной системы должен руководствоваться целями защиты информации, определенными в законодательных актах и политике информационной безопасности.

15. При проектировании системы защиты информации информационной системы, функционирование которой предполагается на базе информационной системы другого собственника (владельца), имеющей аттестованную систему защиты информации, может быть предусмотрено применение требований, реализованных в системе защиты информации информационной системы этого собственника (владельца). Такие требования применяются согласно договору на оказание соответствующих услуг.

▶ГЛАВА 3
СОЗДАНИЕ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

16. На этапе создания системы защиты информации осуществляется реализация мер по технической и криптографической защите информации, в том числе:

внедрение средств защиты информации, проверка их работоспособности и совместимости с активами информационной системы;

корректировка (при необходимости) разработанных на этапе проектирования системы защиты информации структурной и логической схем информационной системы;

корректировка (при необходимости) разработанных на этапе проектирования системы защиты информации проектов локальных правовых актов и других организационно-распорядительных документов по вопросам применения системы защиты информации и их утверждение.

17. В ходе внедрения средств технической и криптографической защиты информации осуществляются:

их монтаж и наладка в соответствии с проектами локальных правовых актов и других организационно-распорядительных документов по вопросам применения системы защиты информации, рекомендациями изготовителей, ограничениями, установленными в сертификатах соответствия, требованиями по совместимости средств криптографической защиты информации;

проверка корректности выполнения такими средствами требований по защите информации в реальных условиях эксплуатации и во взаимодействии с активами

информационной системы. В рамках такой проверки допускается обработка только общедоступной информации;

маркировка всех физических линий связи согласно структурной схеме информационной системы.

18. При корректировке разработанных на этапе проектирования системы защиты информации проектов локальных правовых актов и других организационно-распорядительных документов по вопросам применения системы защиты информации учитываются результаты внедрения средств технической и криптографической защиты информации, проверки их работоспособности и совместимости с активами информационной системы.

ГЛАВА 4
ОСОБЕННОСТИ ЭКСПЛУАТАЦИИ ИНФОРМАЦИОННОЙ СИСТЕМЫ С ПРИМЕНЕНИЕМ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

19. В процессе эксплуатации информационной системы с применением аттестованной в установленном порядке системы защиты информации подразделение защиты информации или иное подразделение (должностное лицо), ответственное за обеспечение защиты информации:

реализует регламентированные в локальных правовых актах и других организационно-распорядительных документах по вопросам применения системы защиты информации меры по защите информации;

реализует мероприятия по выявлению угроз, которые могут привести к сбоям, нарушению функционирования информационной системы, реагированию на соответствующие события и ликвидации их последствий;

при выявлении событий, которые фактически угрожают конфиденциальности, целостности, подлинности, доступности и сохранности информации или представляют собой нарушение политики информационной безопасности, проводит на внеплановой основе мероприятия, предусмотренные в абзаце десятом настоящей части;

осуществляет контроль за соблюдением у собственника (владельца) информационной системы требований, установленных законодательством, локальными правовыми актами и другими организационно-распорядительными документами по вопросам применения системы защиты информации;

принимает меры, направленные на совершенствование системы защиты информации;

при заключении и исполнении собственником (владельцем) информационной системы договоров с юридическими и физическими лицами по вопросам обеспечения функционирования, модернизации информационной системы участвует в проведении наладочных работ и сервисного (технического) обслуживания активов информационной системы, средств защиты информации;

на регулярной основе, но не реже одного раза в год со дня аттестации системы защиты информации проводит:

инструктажи, иные мероприятия, направленные на повышение уровня знаний и навыков работников собственника (владельца) информационной системы по вопросам применения системы защиты информации в части, их касающейся;

анализ эффективности применения системы защиты информации, включая пересмотр применяемых мер по защите информации на предмет их актуальности и необходимости внесения изменений в систему защиты информации.

Результаты проведения мероприятий, предусмотренных в абзаце десятом части первой настоящего пункта, должны быть отражены в документе произвольной формы, который подлежит утверждению руководителем организации – собственника (владельца) информационной системы.

20. В случае невозможности устранения выявленных в процессе эксплуатации информационной системы нарушений ее функционирования в течение пяти рабочих дней

с момента выявления таких нарушений собственник (владелец) информационной системы обязан прекратить обработку информации, распространение и (или) предоставление которой ограничено, о чем письменно проинформировать ОАЦ.

В случае компрометации криптографических ключей средств криптографической защиты информации собственник (владелец) информационной системы обязан незамедлительно прекратить использование данных средств для обработки информации.

21. При получении собственником (владельцем) информационной системы от физического лица его персональных данных, предоставленных этим физическим лицом без использования средств криптографической защиты информации, предоставление в последующем этих персональных данных тем же собственником (владельцем) информационной системы названному физическому лицу может осуществляться без использования средств криптографической защиты информации.

22. При наличии нескольких введенных в эксплуатацию информационных систем собственник (владелец) этих информационных систем обязан утвердить и поддерживать в актуальном состоянии перечень таких систем с указанием в нем присвоенных этим системам соответствующих классов типовых информационных систем.

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

24. В случае прекращения эксплуатации информационной системы собственник (владелец) информационной системы в соответствии с локальными правовыми актами и другими организационно-распорядительными документами по вопросам применения системы защиты информации принимает меры по:

защите информации, которая обрабатывалась в информационной системе;

резервному копированию информации и криптографических ключей (при необходимости), обеспечению их конфиденциальности и целостности;

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

Приложение 1
к Положению о порядке технической
и криптографической защиты информации
в информационных системах, предназначенных
для обработки информации, распространение
и (или) предоставление которой ограничено
(в редакции приказа
Оперативно-аналитического центра
при Президенте Республики Беларусь
10.12.2024 № 259)

КЛАССЫ
типовых информационных систем

1. Класс 4-ин – информационные системы, в которых обрабатываются персональные данные, за исключением специальных персональных данных, и которые не имеют подключений к сетям электросвязи общего пользования (открытым каналам передачи данных) (далее – открытые каналы передачи данных).

2. Класс 4-спец – информационные системы, в которых обрабатываются специальные персональные данные, за исключением биометрических и генетических персональных данных, и которые не имеют подключений к открытым каналам передачи данных.

3. Класс 4-бг – информационные системы, в которых обрабатываются биометрические и генетические персональные данные и которые не имеют подключений к открытым каналам передачи данных.

4. Класс 4-юл – информационные системы, в которых обрабатывается информация, составляющая коммерческую и иную охраняемую законом тайну юридического лица, распространение и (или) предоставление которой ограничено (за исключением сведений, составляющих государственные секреты, и служебной информации ограниченного распространения), и которые не имеют подключений к открытым каналам передачи данных.

5. Класс 4-дсп – информационные системы, в которых обрабатывается служебная информация ограниченного распространения и которые не имеют подключений к открытым каналам передачи данных.

6. Класс 3-ин – информационные системы, в которых обрабатываются персональные данные, за исключением специальных персональных данных, и которые подключены к открытым каналам передачи данных.

7. Класс 3-спец – информационные системы, в которых обрабатываются специальные персональные данные, за исключением биометрических и генетических персональных данных, и которые подключены к открытым каналам передачи данных.

8. Класс 3-бг – информационные системы, в которых обрабатываются биометрические и генетические персональные данные и которые подключены к открытым каналам передачи данных.

9. Класс 3-юл – информационные системы, в которых обрабатывается информация, составляющая коммерческую и иную охраняемую законом тайну юридического лица, распространение и (или) предоставление которой ограничено (за исключением сведений, составляющих государственные секреты, и служебной информации ограниченного распространения), и которые подключены к открытым каналам передачи данных.

10. Класс 3-дсп – информационные системы, в которых обрабатывается служебная информация ограниченного распространения и которые подключены к открытым каналам передачи данных.

Приложение 2
к Положению о порядке технической
и криптографической защиты информации
в информационных системах, предназначенных
для обработки информации, распространение
и (или) предоставление которой ограничено
(в редакции приказа
Оперативно-аналитического центра
при Президенте Республики Беларусь
10.12.2024 № 259)

Форма

УТВЕРЖДАЮ

_____
(наименование должности
руководителя организации)

_____
(подпись, инициалы, фамилия)
__.__.20__

АКТ
отнесения информационной системы к классу (классам)
типовых информационных систем

_____
(наименование и место нахождения организации)

Настоящий акт составлен комиссией, назначенной _____
(вид документа)
от ___.__.20___ № _____, в составе:
председателя _____,
членов комиссии: _____
о том, что в информационной системе _____,
(полное наименование информационной системы)
которая _____ к сетям электросвязи общего пользования
(подключена или не подключена)
(открытым каналам передачи данных) и в которой будет (будут) обрабатываться
_____
(указывается вид информации, распространение и (или) предоставление которой ограничено, согласно части
_____,
первой статьи 17 Закона Республики Беларусь «Об информации, информатизации и защите информации»)
присвоен (присвоены) класс (классы) _____.

Председатель комиссии _____ _____
(подпись) (инициалы, фамилия)

Члены комиссии: _____ _____
(подпись) (инициалы, фамилия)

_____ _____
(подпись) (инициалы, фамилия)

Приложение 3
к Положению о порядке технической
и криптографической защиты информации
в информационных системах, предназначенных
для обработки информации, распространение
и (или) предоставление которой ограничено
(в редакции приказа
Оперативно-аналитического центра
при Президенте Республики Беларусь
10.12.2024 № 259)

ПЕРЕЧЕНЬ
требований к системе защиты информации, подлежащих включению в техническое задание

	Наименование требований	Классы типовых информационных систем							
		4-ин, 4-спец	4-бг	4-юл	4-дсп	3-ин, 3-спец	3-бг	3-юл	3-дсп
1	Аудит безопасности:								
1.1	определение состава сведений о событиях информационной безопасности, подлежащих регистрации	+	+	+	+	+	+	+	+
1.2	обеспечение сбора и хранения сведений о событиях информационной безопасности в течение установленного срока хранения, но не менее одного года	+	+	+	+	+	+	+	+
1.3	обеспечение централизованного сбора и хранения сведений о событиях информационной безопасности в течение установленного срока хранения, но не менее одного года	+/–	+	+/–	+/–	+	+	+	+
1.4	определение способа (просмотр, анализ) и периодичности мониторинга событий информационной безопасности уполномоченными на это пользователями информационной системы	+	+	+	+	+	+	+	+
1.5	обеспечение сбора и хранения информации о функционировании средств вычислительной техники, телекоммуникационного оборудования и средств защиты информации в течение установленного срока хранения, но не менее одного года	+	+	+	+	+	+	+	+
2	Требования по обеспечению защиты информации:								
2.1	регламентация порядка использования в информационной системе съемных носителей информации, мобильных технических средств и контроля за таким использованием	+	+	+	+	+	+	+	+
2.2	обеспечение контроля за работоспособностью, параметрами настройки и правильностью функционирования средств вычислительной техники, телекоммуникационного оборудования, системного программного обеспечения и средств защиты информации	+	+	+	+	+	+	+	+
2.3	обеспечение защиты от несанкционированного доступа к резервным копиям, параметрам настройки телекоммуникационного оборудования, системного программного обеспечения, средств защиты информации и событиям безопасности	+	+	+	+	+	+	+	+
3	Требования по обеспечению идентификации и аутентификации:								
3.1	обеспечение разграничения доступа пользователей к средствам вычисли-тельной	+	+	+	+	+	+	+	+

	техники, телекоммуникационному оборудованию, системному и прикладному программному обеспечению и средствам защиты информации								
3.2	обеспечение идентификации и аутентификации пользователей активов информационной системы, средств защиты информации	+	+	+	+	+	+	+	+
3.3	обеспечение защиты обратной связи при вводе аутентификационной информации	+	+	+	+	+	+	+	+
3.4	обеспечение полномочного управления (создание, активация, блокировка и уничтожение) учетными записями пользователей информационной системы	+	+	+	+	+	+	+	+
3.5	обеспечение контроля за соблюдением правил генерации и смены паролей пользователей информационной системы	+	+	+	+	+	+	+	+
3.6	обеспечение централизованного управления учетными записями пользователей информационной системы	+/–	+/–	+/–	+/–	+/–	+	+	+
3.7	обеспечение блокировки доступа к активам информационной системы, средствам защиты информации после истечения установленного времени бездействия (неактивности) пользователя информационной системы или по его запросу	+	+	+	+	+	+	+	+
4	Требования по защите системы защиты информации информационной системы:								
4.1	изменение установленных по умолчанию реквизитов доступа к активам информационной системы, средствам защиты информации либо блокирование возможности их использования	+	+	+	+	+	+	+	+
4.2	обеспечение замены или модернизации активов информационной системы, средств защиты информации после истечения установленного для них срока эксплуатации, за исключением случаев, влекущих прекращение функционирования этих активов и средств	+	+	+	+	+	+	+	+
4.3	обеспечение контроля и управления физическим доступом в помещения, в которых постоянно размещаются активы информационной системы, средства защиты информации	+	+	+	+	+	+	+	+
4.4	синхронизация системного времени активов информационной системы, средств защиты информации от единого (общего) источника	+	+	+	+	+	+	+	+
5	Обеспечение криптографической защиты информации:								
5.1	обеспечение конфиденциальности и контроля целостности информации при ее передаче посредством сетей электросвязи общего пользования (открытых каналов передачи данных) (средства линейного шифрования и (или) предварительного шифрования)	+/–	+/–	+/–	+/–	+	+	+	+
5.2	обеспечение конфиденциальности и контроля целостности информации при ее хранении в информационной системе (средства предварительного шифрования)	+/–	+	+/–	+/–	+/–	+	+/–	+/–
5.3	обеспечение подлинности и контроля целостности электронных документов в информационной системе (средства электронной цифровой подписи)	+	+	+	+	+	+	+	+
5.4	обеспечение контроля целостности информации в информационной системе (средства контроля целостности)	+/–	+	+/–	+/–	+/–	+	+/–	+/–

5.5	обеспечение конфиденциальности и контроля целостности личных ключей, используемых при выработке электронной цифровой подписи (криптографический токен и (или) средства выработки электронной цифровой подписи)	+	+	+	+	+	+	+	+
5.6	обеспечение многофакторной и (или) многоэтапной аутентификации пользователей в информационной системе (криптографический токен и (или) средства выработки электронной цифровой подписи)	+/–	+/–	+/–	+/–	+/–	+/–	+/–	+/–
5.7	издание сертификатов открытых ключей проверки электронной цифровой подписи (удостоверяющий центр, регистрационный центр (при его наличии), средства электронной цифровой подписи)	+	+	+	+	+	+	+	+
6	Дополнительные требования по обеспечению защиты информации в виртуальной инфраструктуре:								
6.1	обеспечение защиты от агрессивного использования ресурсов виртуальной инфраструктуры потребителями услуг	+/–	+/–	+/–	+/–	+	+	+	+
6.2	обеспечение защиты виртуальной инфраструктуры от несанкционированного доступа и сетевых атак из виртуальной и (или) физической сети, а также виртуальных машин	+/–	+/–	+/–	+/–	+	+	+	+
6.3	обеспечение безопасного перемещения виртуальных машин и обрабатываемой на них информации	+	+	+	+	+	+	+	+
6.4	обеспечение резервного копирования виртуальных машин	+/–	+	+/–	+	+	+	+	+
6.5	обеспечение резервирования сетевого оборудования по схеме N+1	+/–	+/–	+/–	+/–	+/–	+/–	+	+
6.6	физическая изоляция сегмента виртуальной инфраструктуры (система хранения и обработки информации), предназначенного для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам	+/–	+/–	+/–	+	+/–	+/–	+/–	+
7	Иные требования:								
7.1	определение перечня разрешенного программного обеспечения и регламентация порядка его установки и использования	+	+	+	+	+	+	+	+
7.2	обеспечение контроля за составом активов информационной системы, средств защиты информации	+	+	+	+	+	+	+	+
7.3	автоматизированный контроль за составом активов информационной системы, средств защиты информации	+/–	+/–	+/–	+/–	+/–	+	+	+
7.4	использование активов информационной системы под пользовательскими учетными записями (использование учетных записей, имеющих административные привилегии, только в случае управления активами информационной системы или наличия особенностей функционирования активов информационной системы)	+	+	+	+	+	+	+	+
7.5	определение состава и содержания информации, подлежащей резервному копированию	+	+	+	+	+	+	+	+
7.6	обеспечение резервного копирования информации	+	+	+	+	+	+	+	+
7.7	обеспечение резервного копирования конфигурационных файлов телекоммуникационного оборудования	+/–	+	+/–	+	+	+	+	+
7.8	обеспечение обновления программного обеспечения и контроля за своевременностью	+	+	+	+	+	+	+	+

	такого обновления, за исключением случаев, влекущих прекращение функционирования этих активов и средств								
7.9	обеспечение сегментирования (изоляции) сети управления активами информационной системы, средствами защиты информации от сети передачи данных	+/–	+/–	+/–	+/–	+	+	+	+
7.10	обеспечение защиты от воздействия вредоносных программ	+	+	+	+	+	+	+	+
7.11	обеспечение управления информационными потоками (внутренними и внешними) (маршрутизация), использование маршрутизатора (коммутатора маршрутизирующего)	+/–	+/–	+/–	+/–	+	+	+	+
7.12	обеспечение межсетевого экранирования при информационном взаимодействии (внутреннем и внешнем) по протоколам сетевого и транспортного уровней	+/–	+/–	+/–	+/–	+	+	+	+
7.13	обеспечение обнаружения и предотвращения вторжений при информационном взаимодействии (внутреннем и внешнем)	+/–	+/–	+/–	+/–	+	+	+	+
7.14	обеспечение обнаружения и предотвращения вторжений в информационной системе при использовании в ней беспроводных каналов передачи данных (Wi-Fi и (или) др.)	+/–	+/–	+/–	+/–	+	+	+	+
7.15	обеспечение обнаружения и предотвращения утечек информации из информационной системы, использование системы обнаружения утечек информации из информационной системы	+/–	+/–	+/–	+/–	+/–	+/–	+/–	+
7.16	обеспечение контроля за внешними подключениями к информационной системе	+/–	+/–	+/–	+/–	+	+	+	+
7.17	ежегодное проведение оценки эффективности защищенности информационной системы (тестирование на проникновение)	+/–	+/–	+/–	+/–	+/–	+	+/–	+
7.18	обеспечение обнаружения и реагирования на угрозы безопасности конечных узлов (уровня узла) в информационной системе	+/–	+/–	+/–	+/–	+/–	+	+/–	+
7.19	обеспечение централизованного сбора и хранения сведений о DNS-запросах активов информационной системы, средств защиты информации в течение установленного срока хранения, но не менее одного месяца	+/–	+/–	+/–	+/–	+	+	+	+

Примечания:

1. Обозначения «4-ин», «4-спец», «4-бг», «4-юл», «4-дсп», «3-ин», «3-спец», «3-бг», «3-юл» и «3-дсп» соответствуют классам типовых информационных систем.

2. Требования, отмеченные знаком «+», являются обязательными.

3. Требования, отмеченные знаком «+/–», являются рекомендуемыми.

Приложение 4
к Положению о порядке технической
и криптографической защиты информации
в информационных системах, предназначенных
для обработки информации, распространение
и (или) предоставление которой ограничено
(в редакции приказа
Оперативно-аналитического центра
при Президенте Республики Беларусь
10.12.2024 № 259)

МЕТОДЫ
обезличивания персональных данных

1. Для обезличивания персональных данных используются следующие методы:
введение идентификаторов;
изменение состава;
декомпозиция;
перестановка.

2. Метод введения идентификаторов реализуется путем замены персональных данных или части персональных данных, позволяющих идентифицировать субъекта персональных данных, их идентификаторами и создания таблицы соответствия с последующим раздельным хранением идентификаторов и таблиц.

3. Метод изменения состава реализуется путем обобщения, изменения или удаления части сведений, позволяющих идентифицировать субъекта персональных данных, с последующим раздельным хранением полученных персональных данных и правил изменения.

4. Метод декомпозиции реализуется путем разбиения множества записей персональных данных на несколько подмножеств и создания таблиц, устанавливающих связи между подмножествами, с последующим раздельным хранением подмножеств и таблиц.

Для реализации метода декомпозиции необходимо предварительно разработать правила разбиения множества записей на подмножества, правила установления соответствия между записями в различных таблицах и правила внесения изменений в подмножества и таблицы.

5. Метод перестановки реализуется путем взаимного перемещения отдельных записей и (или) групп записей с последующим раздельным хранением полученных персональных данных и правил изменения.

УТВЕРЖДЕНО

Приказ
Оперативно-аналитического центра
при Президенте Республики Беларусь
20.02.2020 № 66
(в редакции приказа
Оперативно-аналитического центра
при Президенте Республики Беларусь
10.12.2024 № 259)

ПОЛОЖЕНИЕ
о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено

1. В настоящем Положении в соответствии с абзацем третьим подпункта 6.4 пункта 6 Положения о технической и криптографической защите информации, утвержденного Указом Президента Республики Беларусь от 16 апреля 2013 г. № 196, определяется порядок аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам (далее – информационная система).

Настоящее Положение может не применяться:

собственниками (владельцами) информационных систем, в которых обрабатываются только общедоступные персональные данные и (или) персональные данные, полученные после применения методов обезличивания, – в отношении таких информационных систем;

операторами электросвязи – собственниками (владельцами) информационных систем, обеспечивающих управление технологическими процессами и предназначенных только для передачи персональных данных по технологическим сетям электросвязи, – в отношении таких информационных систем. Для целей применения настоящего абзаца операторы электросвязи согласовывают с Оперативно-аналитическим центром при Президенте Республики Беларусь (далее – ОАЦ) перечни указанных информационных систем, к которым должны прилагаться структурная и логическая схемы каждой информационной системы, включенной в перечень.

2. Для целей настоящего Положения термины используются в значениях, определенных в Положении о технической и криптографической защите информации, Законе Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации», Законе Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных», 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 соответствие системы защиты информации требованиям законодательства об информации, информатизации и защите информации;

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

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

Собственники (владельцы) информационных систем вправе самостоятельно проводить аттестацию.

4. При проведении аттестации собственником (владельцем) информационной системы самостоятельно работы по аттестации выполняются комиссией, назначенной решением (приказом, иным документом) руководителя собственника (владельца) информационной системы. Физические лица, являющиеся собственниками

информационных систем, в которых обрабатываются персональные данные, вправе выполнять работы по аттестации единолично.

Аттестация специализированными организациями проводится на основании сведений, содержащихся:

в акте отнесения информационной системы к классу (классам) типовых информационных систем;

в политике информационной безопасности;

в структурной и логической схемах информационной системы;

в техническом задании на создание информационной системы или системы защиты информации*;

в локальных правовых актах и других организационно-распорядительных документах по вопросам применения системы защиты информации;

в сертификатах соответствия либо экспертных заключениях на средства защиты информации.

При проведении аттестации специализированной организацией привлекаются представители собственника (владельца) информационной системы из состава подразделения защиты информации или иного подразделения (должностное лицо), ответственного (ответственное) за обеспечение защиты информации.

---

* Техническое задание на создание информационной системы представляется в случае закрепления в нем требований по защите информации.

5. Аттестация проводится:

при создании или модернизации системы защиты информации;

в случае истечения срока действия аттестата соответствия;

в случае изменения технологии обработки защищаемой информации и (или) технических мер, реализованных при создании или модернизации системы защиты информации.

Дополнительные основания для проведения аттестации (помимо случаев, определенных в части первой настоящего пункта) могут предусматриваться собственником (владельцем) информационной системы.

6. Аттестация 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:

разработку программы и методики аттестации;

проверку правильности отнесения информационной системы к классу (классам) типовых информационных систем;

установление соответствия фактического состава активов информационной системы структурной и логической схемам информационной системы;

проверку достаточности реализованных в системе защиты информации мер по защите информации, в том числе:

анализ локальных правовых актов и других организационно-распорядительных документов по вопросам применения системы защиты информации на предмет их соответствия требованиям законодательства об информации, информатизации и защите информации;

проведение испытаний системы защиты информации на предмет выполнения установленных законодательством требований по защите информации;

внешнюю и внутреннюю проверку отсутствия либо невозможности использования нарушителем свойств активов информационной системы, средств защиты информации, которые могут быть случайно инициированы (активированы) или умышленно использованы для нарушения безопасности системы и сведения о которых подтверждены изготовителями (разработчиками) этих активов информационной системы, средств защиты информации;

оценку эффективности защищенности информационной системы классов «3-бг» и (или) «3-дсп» (тестирование на проникновение);

оформление технического отчета и протокола испытаний;

оформление аттестата соответствия.

Допускается выполнение мероприятий по аттестации на выделенном наборе сегментов информационной системы, обеспечивающих полную реализацию технологии обработки защищаемой информации.

При аттестации информационных систем классов «3-ин», «3-спец», «3-бг», «3-юл» и «3-дсп» мероприятия, предусмотренные в абзацах восьмом и девятом части первой настоящего пункта, проводятся с использованием средств оценки эффективности защищенности (средств тестирования на проникновение) (сетевой сканер, сканер уязвимостей, сканер уязвимостей веб-приложений).

Мероприятия, предусмотренные в абзацах втором–десятом части первой настоящего пункта, могут не проводиться при соблюдении в совокупности следующих условий:

аттестация системы защиты информации информационной системы, создаваемой на базе информационной системы специализированной организации, проводится этой специализированной организацией;

в системе защиты информации информационной системы специализированной организации, аттестованной в установленном порядке, реализованы требования по защите информации аттестуемой системы защиты информации.

9. Программа и методика аттестации разрабатываются на основании сведений, указанных в части второй пункта 4 настоящего Положения, и должны содержать перечень выполняемых работ с указанием ответственных лиц, сроков выполнения этих работ, описанием используемых методов проверки требований, реализованных в системе защиты информации, перечень используемых контрольных средств.

Программа и методика аттестации разрабатываются:

комиссией, назначенной решением (приказом, иным документом) руководителя собственника (владельца) информационной системы, – при проведении аттестации собственником (владельцем) информационной системы самостоятельно. Физические лица, являющиеся собственниками информационных систем, в которых обрабатываются персональные данные, вправе разработать программу и методику аттестации единолично;

специализированной организацией – при проведении аттестации такой организацией. В данном случае специализированная организация согласовывает разработанные программу и методику аттестации с собственником (владельцем) информационной системы.

10. Протокол испытаний должен содержать подробное описание проведенных мероприятий, в том числе с применением графических изображений, позволяющее сформировать вывод о полноте выполнения мероприятий, предусмотренных в части первой пункта 8 настоящего Положения.

11. Технический отчет должен содержать:

наименование информационной системы с указанием присвоенного (присвоенных) ей класса (классов) типовых информационных систем;

требования к системе защиты информации согласно приложению 3 к Положению о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденному приказом, утверждающим настоящее Положение, с описанием компенсирующих мер (в случае согласования таких мер с ОАЦ);

сведения об организации информационного взаимодействия с иными информационными системами, если предполагается такое взаимодействие;

сведения о выполнении требований безопасности средств криптографической защиты информации, которые должны соблюдаться при их эксплуатации в соответствии с выбранным уровнем безопасности;

порядок обезличивания персональных данных, если предполагается обезличивание персональных данных;

требования из числа реализованных в аттестованной в установленном порядке системе защиты информации информационной системы другого собственника (владельца),

если функционирование информационной системы, система защиты информации которой проходит аттестацию, предполагается на базе информационной системы другого собственника (владельца) в соответствии с пунктом 15 Положения о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденного приказом, утверждающим настоящее Положение;

список лиц, проводивших испытания, и сроки проведения;

отчет о внешней и внутренней проверке отсутствия либо невозможности использования нарушителем свойств активов информационной системы, средств защиты информации, которые могут быть случайно инициированы (активированы) или умышленно использованы для нарушения безопасности системы и сведения о которых подтверждены изготовителями (разработчиками) этих активов информационной системы, средств защиты информации;

отчет об оценке эффективности защищенности информационной системы классов «3-бг» и (или) «3-дсп» (тестировании на проникновение);

выводы о соответствии (несоответствии) фактического состава активов информационной системы структурной и логической схемам информационной системы, выполнении (невыполнении) установленных законодательством требований по защите информации.

12. Срок проведения аттестации:

определяется руководителем собственника (владельца) информационной системы, физическим лицом, являющимся собственником информационной системы, в которой обрабатываются персональные данные, – при проведении аттестации собственником (владельцем) информационной системы самостоятельно;

не может превышать 180 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 собственнику (владельцу) информационной системы соответствующее уведомление. Собственник (владелец) информационной системы должен устранить недостатки, выявленные указанной организацией, в течение 30 календарных дней со дня получения уведомления. При невозможности устранения собственником (владельцем) информационной системы выявленных недостатков в указанный срок специализированная организация отказывает в выдаче аттестата соответствия. После устранения недостатков собственник (владелец) информационной системы вправе повторно обратиться за проведением аттестации в порядке, установленном настоящим Положением.

13. При подтверждении соответствия системы защиты информации требованиям законодательства об информации, информатизации и защите информации оформляется аттестат соответствия по форме согласно приложению, который подписывается:

руководителем собственника (владельца) информационной системы, физическим лицом, являющимся собственником информационной системы, в которой обрабатываются персональные данные, – при проведении аттестации собственником (владельцем) информационной системы самостоятельно;

руководителем специализированной организации – при проведении аттестации специализированной организацией.

Аттестат соответствия оформляется сроком на пять лет.

Приложение
к Положению о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено
(в редакции приказа Оперативно-аналитического центра при Президенте Республики Беларусь 10.12.2024 № 259)

Форма

АТТЕСТАТ СООТВЕТСТВИЯ
системы защиты информации информационной системы требованиям по защите информации

от __ _____ 20__ г. № _____

Настоящим аттестатом соответствия подтверждается, что система защиты информации

_____
(наименование информационной системы)

_____
(наименование собственника (владельца) информационной системы)

класса (классов) _____ соответствует требованиям по защите
(класс (классы) типовых информационных систем)

информации, предусмотренным законодательством и _____.
(наименование документов)

Аттестация проведена в соответствии с программой, утвержденной __ _____ 20__ г., и методикой, утвержденной __ _____ 20__ г.

Результаты испытаний приведены в протоколе испытаний от ___ _____ 20__ г.

При эксплуатации информационной системы запрещается:

_____.
(при необходимости указываются ограничения на обработку информации)

Аттестат соответствия действителен до ___ _____ 20___ г.

_____	_____	_____
(информация о лице, проводившем аттестацию*)	(подпись)	(инициалы, фамилия)

_____

* Должность с указанием наименования организации – собственника (владельца) информационной системы или специализированной организации. При оформлении аттестата физическим лицом, осуществляющим индивидуальную предпринимательскую деятельность, указывается его статус, иным физическим лицом – предусматривается запись «Собственник информационной системы».

УТВЕРЖДЕНО

Приказ
Оперативно-аналитического
центра при Президенте
Республики Беларусь
20.02.2020 № 66

ПОЛОЖЕНИЕ
о порядке технической и криптографической защиты информации, обрабатываемой на критически важных объектах информатизации

1. В настоящем Положении в соответствии с абзацем четвертым подпункта 6.4 пункта 6 Положения о технической и криптографической защите информации определяется порядок технической и криптографической защиты информации, обрабатываемой на критически важных объектах информатизации, в том числе порядок проектирования, создания и аудита систем информационной безопасности критически важных объектов информатизации (далее – системы информационной безопасности).

Требования по технической и криптографической защите информации, предусмотренные настоящим Положением, реализуются также на критически важных объектах информатизации, являющихся информационными системами, имеющими аттестованную в установленном порядке систему защиты информации.

2. Для целей настоящего Положения термины используются в значениях, определенных в Положении о технической и криптографической защите информации, Положении о порядке отнесения объектов информатизации к критически важным объектам информатизации, утвержденном Указом Президента Республики Беларусь от 16 апреля 2013 г. № 196, и Законе Республики Беларусь «Об информации, информатизации и защите информации».

3. Системы информационной безопасности создаются владельцами критически важных объектов информатизации и включают совокупность правовых, организационных и технических мер, направленных на обеспечение информационной безопасности критически важных объектов информатизации.

4. Система информационной безопасности должна обеспечивать:

предотвращение неправомерного доступа к информации, обрабатываемой на критически важном объекте информатизации, уничтожения такой информации, ее модификации, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации;

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, в том числе за счет создания и хранения резервных копий информации.

5. Владелец критически важного объекта информатизации организует и контролирует функционирование системы информационной безопасности, определяет ее состав и структуру, функции ее участников при обеспечении информационной безопасности критически важного объекта информатизации в зависимости от количества таких объектов и (или) особенностей деятельности владельца критически важного объекта информатизации.

6. Для проведения работ по технической и криптографической защите информации, обрабатываемой на критически важном объекте информатизации, владелец такого объекта создает подразделение защиты информации или назначает уполномоченное должностное лицо (далее – подразделение защиты информации (должностное лицо). Работники такого подразделения (должностное лицо) должны иметь высшее образование в области защиты информации либо высшее, или среднее специальное, или профессионально-техническое

образование и пройти переподготовку или повышение квалификации по вопросам технической и криптографической защиты информации в порядке, установленном законодательством.

7. В случае невозможности выполнения работ по технической и криптографической защите информации, обрабатываемой на критически важном объекте информатизации, силами подразделения защиты информации (должностным лицом) руководителем организации могут привлекаться организации, имеющие лицензии на осуществление деятельности по технической и (или) криптографической защите информации в части соответствующих составляющих данный вид деятельности работ и (или) услуг (далее – специализированные организации).

8. Подразделение защиты информации (должностное лицо):

разрабатывает проекты локальных правовых актов по созданию и совершенствованию системы информационной безопасности;

проводит анализ угроз и расчет рисков информационной безопасности критически важного объекта информатизации;

обеспечивает в соответствии с требованиями по информационной безопасности критически важного объекта информатизации реализацию необходимых организационных и технических мер, а также применение и эксплуатацию средств защиты информации;

осуществляет мониторинг и реагирование на возникновение рисков информационной безопасности критически важного объекта информатизации;

организует проведение аудита системы информационной безопасности;

согласовывает прием на работу, увольнение, перевод, перемещение работников, трудовые обязанности которых предусматривают эксплуатацию активов критически важного объекта информатизации, с учетом требований по информационной безопасности критически важного объекта информатизации;

проводит инструктажи, мероприятия по информированию и выработке практических навыков действий по обеспечению информационной безопасности критически важного объекта информатизации;

обеспечивает защиту сведений, содержащихся в эксплуатационной документации на критически важный объект информатизации, документации на систему информационной безопасности, иной информации, распространение и (или) предоставление которой ограничено, от ее разглашения или несанкционированного доступа к ней со стороны третьих лиц;

обеспечивает взаимодействие владельца критически важного объекта информатизации с юридическими и физическими лицами при заключении и исполнении договоров по вопросам обеспечения информационной безопасности критически важного объекта информатизации.

Обязанности, возлагаемые на подразделение защиты информации (должностное лицо), должны быть определены в локальных правовых актах владельца критически важного объекта информатизации. Не допускается возложение на подразделение защиты информации (должностное лицо) функций, не связанных с обеспечением технической и криптографической защиты информации.

9. Подразделение защиты информации (должностное лицо) реализует функции, предусмотренные в части первой пункта 8 настоящего Положения, во взаимодействии с иными подразделениями (работниками), обеспечивающими функционирование и эксплуатацию активов критически важного объекта информатизации.

Объем задач, возлагаемых на подразделения (работников), обеспечивающие функционирование и эксплуатацию активов критически важного объекта информатизации, определяется владельцем критически важного объекта информатизации в локальных правовых актах по вопросам технической и криптографической защиты информации, обрабатываемой на критически важном объекте информатизации.

Положения локальных правовых актов по вопросам технической и криптографической защиты информации, обрабатываемой на критически важном объекте информатизации, доводятся до сведения работников, обеспечивающих функционирование и эксплуатацию активов критически важного объекта информатизации, в части, их касающейся.

10. Владельцы критически важных объектов информатизации не реже одного раза в год обеспечивают проведение мероприятий, направленных на повышение уровня знаний работников по вопросам информационной безопасности критически важных объектов информатизации, информирование о возможных рисках и угрозах информационной безопасности критически важных объектов информатизации.

11. Представители организаций, привлекаемых владельцем критически важного объекта информатизации для выполнения работ на таких объектах, должны быть ознакомлены с требованиями локальных правовых актов по вопросам технической и криптографической защиты информации, обрабатываемой на критически важном объекте информатизации, в части, их касающейся.

12. При осуществлении технической и криптографической защиты информации, обрабатываемой на критически важных объектах информатизации, 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 Оперативно-аналитическим центром при Президенте Республики Беларусь.

Параметры и характеристики применяемых средств защиты информации должны реализовывать технические меры по обеспечению информационной безопасности критически важного объекта информатизации.

Применяемые средства защиты информации должны быть обеспечены гарантийной и технической поддержкой со стороны изготовителей (разработчиков) этих средств. При выборе средств защиты информации должно учитываться возможное наличие ограничений со стороны изготовителей (разработчиков) или иных лиц на применение этих средств на любом из критически важных объектов информатизации, принадлежащих владельцу данных объектов.

Порядок применения средств защиты информации определяется в локальных правовых актах по вопросам технической и криптографической защиты информации, обрабатываемой на критически важном объекте информатизации.

13. В локальных правовых актах по вопросам технической и криптографической защиты информации, обрабатываемой на критически важных объектах информатизации, должны быть также определены порядок и правила функционирования системы информационной безопасности, в том числе:

цели и задачи обеспечения информационной безопасности критически важных объектов информатизации, перечень основных угроз и нарушителей информационной безопасности критически важных объектов информатизации, основные организационные и технические меры, проводимые владельцем критически важного объекта информатизации, состав и структура системы информационной безопасности, функции ее участников, порядок применения, форма и порядок проведения аудита;

направления информационной безопасности критически важного объекта информатизации (политика информационной безопасности, формуляр, реестр активов критически важного объекта информатизации, методика оценки рисков, план обработки рисков и другое);

план мероприятий, направленных на повышение уровня знаний работников по вопросам обеспечения информационной безопасности критически важного объекта информатизации и информирование о возможных рисках и угрозах информационной безопасности критически важного объекта информатизации;

порядок реализации организационных и технических мер по обеспечению информационной безопасности критически важного объекта информатизации;

порядок реагирования на возникновение рисков информационной безопасности критически важного объекта информатизации;

порядок взаимодействия подразделений (работников) владельца критически важного объекта информатизации при решении задач обеспечения информационной безопасности критически важного объекта информатизации.

Состав и виды локальных правовых актов по вопросам технической и криптографической защиты информации, обрабатываемой на критически важном объекте информатизации, определяются его владельцем с учетом особенностей его деятельности.

14. Комплекс мероприятий по технической и криптографической защите информации, обрабатываемой на критически важном объекте информатизации, включает проектирование, создание и аудит системы информационной безопасности.

15. На этапе проектирования системы информационной безопасности осуществляются:

15.1. определение внутренних (организационная структура, информационные системы, информационные потоки и процессы) и внешних (взаимосвязи с контрагентами и другое) границ, оказывающих влияние на обеспечение информационной безопасности критически важного объекта информатизации;

15.2. определение целей обеспечения информационной безопасности критически важного объекта информатизации, совместимых с процессами деятельности владельца критически важного объекта информатизации и прогнозными документами организации;

15.3. инвентаризация (выявление и учет), а также определение степени важности для основной деятельности владельца критически важного объекта информатизации (исходя из конфиденциальности, целостности и доступности) следующих активов критически важного объекта информатизации:

программно-аппаратных средств и физических устройств;

программного обеспечения (прикладного и системного);

средств защиты информации;

информационных систем и информационных сетей;

средств обработки информации (потоков информации), средств коммуникации, администрирования и конфигурирования;

15.4. определение работников, ответственных за использование активов критически важного объекта информатизации;

15.5. определение физических и логических границ области применения системы информационной безопасности (формуляр критически важного объекта информатизации) с использованием структурной и логической схем критически важного объекта информатизации. При этом структурная схема должна содержать расположение физических устройств с номерами портов, а также физических линий связи, соединяющих физические интерфейсы технических, программно-аппаратных средств обработки информации, средств защиты информации, автоматизированных рабочих мест администратора (оператора). В логической схеме должны быть отображены информационные системы, направления потоков данных, а также спецификация используемых технологий и протоколов, списки VLAN, IP-адреса устройств;

15.6. определение угроз информационной безопасности критически важного объекта информатизации;

15.7. разработка методологии (методики) оценки рисков информационной безопасности критически важного объекта информатизации и оценка таких рисков;

15.8. определение требований к параметрам настройки программных и программно-аппаратных средств, включая средства защиты информации, по обеспечению информационной безопасности критически важного объекта информатизации, блокированию (нейтрализации) угроз информационной безопасности критически важного объекта информатизации;

15.9. определение средств управления, необходимых для реализации выбранного варианта обработки рисков информационной безопасности критически важного объекта информатизации (план обработки рисков).

16. При создании системы информационной безопасности учитывается ее информационное взаимодействие с иными информационными системами, автоматизированными системами управления технологическими процессами или информационно-телекоммуникационными сетями.

17. Обеспечение информационной безопасности критически важного объекта информатизации достигается путем выполнения совокупности правовых, организационных и технических мер, направленных на блокирование (нейтрализацию) угроз информационной безопасности критически важного объекта информатизации, реализация которых может привести к прекращению или нарушению функционирования этого объекта, обеспечиваемого (управляемого, контролируемого) им процесса, нарушению конфиденциальности, целостности, доступности обрабатываемой информации.

18. Меры по обеспечению информационной безопасности критически важного объекта информатизации определяются и реализуются с учетом угроз информационной безопасности критически важного объекта информатизации на аппаратном, системном, прикладном и сетевом уровнях, в том числе в среде виртуализации.

19. В ходе создания системы информационной безопасности осуществляется разработка политики информационной безопасности критически важного объекта информатизации, содержащая:

приоритетные направления информационной безопасности критически важного объекта информатизации;

перечень требований по информационной безопасности критически важного объекта информатизации и обязательства сотрудников по их выполнению;

организационную структуру системы информационной безопасности;

обязательства по постоянному совершенствованию системы информационной безопасности и выполнению актов законодательства по вопросам технической и криптографической защиты информации, локальных правовых актов.

20. В системе информационной безопасности в зависимости от угроз информационной безопасности критически важного объекта информатизации реализуются следующие организационные и технические меры:

20.1. идентификация и аутентификация:

определение политик и процедур идентификации и аутентификации;

идентификация и аутентификация пользователей и инициируемых ими процессов;

инвентаризация и контроль за активами критически важного объекта информатизации;

20.2. управление доступом к активам критически важного объекта информатизации:

определение политик и процедур управления доступом;

разделение прав доступа пользователей;

управление учетными записями и паролями пользователей;

управление привилегированными правами доступа;

ограничение неуспешных попыток доступа к активам критически важного объекта информатизации;

оповещение пользователя при входе о предыдущем доступе к активам критически важного объекта информатизации;

ограничение числа параллельных сеансов доступа;

блокирование сеанса доступа пользователя при неактивности;

ограничение защищенного удаленного доступа к активам критически важного объекта информатизации;

контроль доступа из внешних информационных (автоматизированных) систем;

использование выделенного автоматизированного рабочего места для администрирования, требующего привилегированного доступа, не имеющего доступа к внешним информационным сетям;

управление запуском, установкой (инсталляцией) компонентов программного обеспечения (приложений);

20.3. обращение с носителями информации:

определение политик и процедур обращения со съемными носителями информации;

учет съемных носителей информации;

управление физическим доступом к съемным носителям информации;

контроль за перемещением съемных носителей информации за пределы контролируемой зоны;

ограничение ввода (вывода) информации на периферийные устройства, в том числе съемные носители информации;

регистрация и контроль за подключением съемных носителей информации;

уничтожение (удаление) информации со съемных носителей информации;

20.4. аудит информационной безопасности:

определение политик и процедур аудита информационной безопасности;

поиск уязвимостей активов критически важного объекта информатизации и их устранение;

генерирование временных меток и (или) синхронизация системного времени;

защита информации о событиях информационной безопасности;

аудит информации о действиях пользователей;

регистрация и мониторинг событий информационной безопасности;

хранение результатов аудита безопасности;

20.5. защита от вредоносного программного обеспечения:

определение политик и процедур защиты от вредоносного программного обеспечения;

реализация защиты от вредоносного программного обеспечения;

обновление механизмов сканирования и базы данных сигнатур вредоносного программного обеспечения;

регистрация событий обнаружения вредоносных программ;

20.6. управление процедурами резервирования:

определение политик и процедур резервирования;

резервирование программных и программно-аппаратных средств и систем;

резервное копирование информации, программного обеспечения и обеспечение возможности восстановления из резервных копий;

резервное копирование конфигурационных файлов и журналов аудита;

обеспечение защиты резервных копий;

20.7. обеспечение информационной безопасности критически важного объекта информатизации и его элементов:

определение политик и процедур защиты информационной (автоматизированной) системы и ее элементов;

разделение функций по управлению активами критически важного объекта информатизации с другими функциями;

сегментирование сети критически важного объекта информатизации;

управление сетевыми потоками;

использование межсетевых экранов;

сокрытие архитектуры и конфигурации критически важного объекта информатизации;

управление безопасной настройкой сетевых устройств (средств защиты информации);

отключение беспроводных соединений и интерфейсов;

исключение доступа через общие ресурсы;

защита от угроз отказа в обслуживании;

ограничение использования мобильных устройств;

управление перемещением виртуальных машин и обрабатываемых на них данных;

20.8. управление конфигурацией:

определение политик и процедур управления конфигурацией информационной (автоматизированной) системы;

идентификация объектов управления конфигурацией;

управление изменениями конфигурации;

установка (инсталляция) только разрешенного к использованию программного обеспечения;

контроль за действиями по изменению конфигурации;

20.9. обновление программного обеспечения:

определение политик и процедур управления обновлениями программного обеспечения;

обновление программного обеспечения из доверенного источника;

20.10. планирование мероприятий по обеспечению информационной безопасности критически важного объекта информатизации:

определение политик и процедур планирования мероприятий по обеспечению информационной безопасности критически важного объекта информатизации;

разработка, утверждение и актуализация плана мероприятий по обеспечению информационной безопасности критически важного объекта информатизации;

контроль за выполнением мероприятий по обеспечению информационной безопасности критически важного объекта информатизации;

20.11. реагирование на события информационной безопасности критически важного объекта информатизации и управление ими:

разработка плана реагирования на события информационной безопасности и его актуализация не реже одного раза в год;

определение периодичности проведения мероприятий по оповещению и отработке действий работников в случае реализации угроз информационной безопасности критически важного объекта информатизации в соответствии с планом реагирования;

разработка и внедрение методологии реагирования на события информационной безопасности, обеспечивающей реагирование в сроки, определенные эксплуатационной документацией на критически важный объект информатизации и локальными правовыми актами, в целях исключения (снижения до приемлемого уровня) вероятного ущерба;

обучение и отработка действий персонала при возникновении событий информационной безопасности;

создание альтернативных мест хранения и обработки информации в случае возникновения событий информационной безопасности;

анализ возникших событий информационной безопасности и принятие мер по недопущению их повторного возникновения;

20.12. информирование и обучение персонала:

определение политик и процедур информирования и обучения персонала, ответственности за нарушение требований по информационной безопасности критически важного объекта информатизации;

информирование персонала об угрозах информационной безопасности критически важного объекта информатизации, правилах безопасной работы с активами критически важного объекта информатизации;

проведение практических занятий с персоналом по правилам безопасной работы;

контроль осведомленности персонала об угрозах информационной безопасности критически важного объекта информатизации и о правилах безопасной работы.

21. В целях постоянного мониторинга угроз безопасности критически важного объекта информатизации владелец этого объекта:

осуществляет постоянный контроль за состоянием активов критически важного объекта информатизации для выявления потенциальных событий информационной безопасности критически важного объекта информатизации;

проводит анализ и оценку угроз информационной безопасности критически важного объекта информатизации;

разрабатывает план восстановления критически важного объекта информатизации, учитывающий события информационной безопасности.

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

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

23. Аудит системы информационной безопасности включает следующие этапы:

анализ и оценку соответствия системы информационной безопасности требованиям настоящего Положения;

проведение контроля эффективности защищенности системы информационной безопасности;

формирование замечаний (недостатков), выявленных в процессе аудита, и предложений по их устранению;

составление акта по форме согласно приложению и рекомендаций по результатам аудита.

24. Акт аудита системы информационной безопасности утверждается:

руководителем владельца критически важного объекта информатизации – в случае проведения аудита системы информационной безопасности подразделением защиты информации (должностным лицом);

руководителем специализированной организации – в случае проведения аудита данной организацией.

Приложение
к Положению о порядке технической
и криптографической защиты информации,
обрабатываемой на критически важных
объектах информатизации
(в редакции приказа
Оперативно-аналитического
центра при Президенте
Республики Беларусь
12.11.2021 № 195)

Форма

Для служебного пользования
Экз. № ___

УТВЕРЖДАЮ
_____
(наименование должности
_____
руководителя организации)
_____
(подпись, инициалы, фамилия)
___.__.20___

АКТ
аудита системы информационной безопасности
критически важного объекта информатизации

_____
(наименование критически важного объекта информатизации)

Вопросы, подлежащие рассмотрению	Отметка о выполнении, номер, дата, наименование документа, в котором реализованы требования
Разработка политики информационной безопасности критически важного объекта информатизации	
Проведение инвентаризации (выявление и учет) активов критически важного объекта информатизации	
Определение работников, ответственных за использование активов критически важного объекта информатизации	
Определение физических и логических границ области применения системы информационной безопасности	
Определение угроз информационной безопасности критически важного объекта информатизации	
Разработка методологии (методики) оценки рисков информационной безопасности критически важного объекта информатизации	
Оценка рисков информационной безопасности критически важного объекта информатизации	
Определение требований к параметрам настройки программных и программно-аппаратных средств, средств защиты информации	
Определение средств управления, необходимых для реализации выбранного варианта обработки рисков безопасности критически важного объекта информатизации (план обработки рисков)	
Идентификация и аутентификация	
Управление доступом к активам критически важного объекта информатизации	
Обращение с носителями информации	

Аудит информационной безопасности	
Защита от вредоносного программного обеспечения	
Управление процедурами резервирования	
Обеспечение информационной безопасности критически важного объекта информатизации и его элементов	
Управление конфигурацией	
Обновление программного обеспечения	
Планирование мероприятий по обеспечению информационной безопасности критически важного объекта информатизации	
Реагирование на события информационной безопасности критически важного объекта информатизации и управление ими	
Информирование и обучение персонала	
Осуществление постоянного контроля за состоянием активов критически важного объекта информатизации в целях выявления событий информационной безопасности критически важного объекта информатизации	
Анализ и оценка угроз информационной безопасности критически важного объекта информатизации	
Разработка плана восстановления критически важного объекта информатизации	

Председатель комиссии _____ _____
(подпись) (инициалы, фамилия)

Члены комиссии: _____ _____
(подпись) (инициалы, фамилия)

_____ _____
(подпись) (инициалы, фамилия)

УТВЕРЖДЕНО

Приказ
Оперативно-аналитического центра
при Президенте Республики Беларусь
20.02.2020 № 66
(в редакции приказа
Оперативно-аналитического центра
при Президенте Республики Беларусь
10.12.2024 № 259)

ПОЛОЖЕНИЕ
о порядке представления в Оперативно-аналитический центр при Президенте Республики Беларусь сведений о событиях информационной безопасности, состоянии технической и криптографической защиты информации

1. В настоящем Положении в соответствии с подпунктами 7.7 и 7.8 пункта 7 Положения о технической и криптографической защите информации, утвержденного Указом Президента Республики Беларусь от 16 апреля 2013 г. № 196, определяется порядок представления в Оперативно-аналитический центр при Президенте Республики Беларусь (далее – ОАЦ) государственными органами и иными организациями – собственниками (владельцами) информационных систем, владельцами критически важных объектов информатизации, организациями, оказывающими услуги по распространению открытых ключей проверки электронной цифровой подписи, указанными в части первой пункта 3 Положения о технической и криптографической защите информации, 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;

о состоянии технической и криптографической защиты информации.

Сведения о событиях информационной безопасности, состоянии технической и криптографической защиты информации в соответствии с настоящим Положением могут не представляться в ОАЦ:

собственниками (владельцами) информационных систем, в которых обрабатываются только общедоступные персональные данные и (или) персональные данные, полученные после применения методов обезличивания, – в отношении таких информационных систем;

операторами электросвязи – собственниками (владельцами) информационных систем, обеспечивающих управление технологическими процессами и предназначенных только для передачи персональных данных по технологическим сетям электросвязи, – в отношении таких информационных систем. Для целей применения настоящего абзаца операторы электросвязи согласовывают с ОАЦ перечни указанных информационных систем, к которым должны прилагаться структурная и логическая схемы каждой информационной системы, включенной в перечень.

2. Для целей настоящего Положения термины используются в значениях, определенных в Положении о технической и криптографической защите информации, Законе Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации», Законе Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных».

3. Владельцы критически важных объектов информатизации представляют в ОАЦ:

3.1. формуляр критически важного объекта информатизации по форме согласно приложению – не позднее пяти рабочих дней после завершения мероприятий по созданию системы информационной безопасности критически важного объекта информатизации и (или) изменения сведений, указанных в формуляре;

3.2. в сроки, определенные в подпункте 3.1 настоящего пункта, посредством получения электронной услуги общегосударственной автоматизированной информационной системы с использованием личных электронных кабинетов, созданных на базе единого портала электронных услуг (далее – личные электронные кабинеты), сведения:

о дате ввода критически важного объекта информатизации в эксплуатацию;

о видах оборудования (коммутатор, маршрутизатор, межсетевой экран, блок управления и др.) и программного обеспечения (операционная система, антивирусное программное обеспечение и др.), входящих в состав активов критически важного объекта информатизации, с указанием их количества, типа (программно-аппаратные средства, физические устройства, программное обеспечение (прикладное, системное), средства защиты информации, средства обработки информации (потоков информации), средства коммуникации, средства администрирования и конфигурирования), даты ввода в эксплуатацию и окончания их поддержки производителем или поставщиком;

3.3. результаты аудита системы информационной безопасности критически важного объекта информатизации – не позднее чем через год после завершения мероприятий по созданию системы информационной безопасности критически важного объекта информатизации и далее ежегодно;

3.4. сведения о событиях информационной безопасности, в том числе о фактах возникновения угроз информационной безопасности критически важного объекта информатизации:

описание источника угрозы информационной безопасности критически важного объекта информатизации и активов критически важного объекта информатизации, на которые она направлена;

условия и причины возникновения угроз информационной безопасности критически важного объекта информатизации.

Сведения, предусмотренные в части первой настоящего подпункта, представляются в произвольной форме в течение суток с момента выявления (обнаружения) соответствующих фактов;

3.5. сведения о планируемом приостановлении функционирования критически важного объекта информатизации (его составляющих элементов) для проведения регламентных, профилактических и иных работ с указанием даты начала и продолжительности таких работ (в произвольной форме).

4. Государственные органы и иные организации – собственники (владельцы) информационных систем, организации, оказывающие услуги по распространению открытых ключей проверки электронной цифровой подписи, указанные в части первой пункта 3 Положения о технической и криптографической защите информации, представляют в ОАЦ:

4.1. сведения об информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам.

Сведения, предусмотренные в части первой настоящего подпункта, представляются не позднее десяти календарных дней со дня оформления (получения) аттестата соответствия системы защиты информации информационной системы требованиям по защите информации и далее не позднее десяти календарных дней с момента изменения ранее представленных сведений;

4.2. сведения о подразделениях защиты информации или иных подразделениях (должностных лицах), ответственных за обеспечение защиты информации, с указанием наименования подразделения, фамилии, собственного имени, отчества (если таковое имеется) должностного лица и работников таких подразделений, полученного ими образования, в том числе переподготовки или повышения квалификации по вопросам технической и криптографической защиты информации, а также контактных данных.

Сведения, предусмотренные в части первой настоящего подпункта, представляются не позднее десяти календарных дней со дня создания (назначения) подразделения

(должностного лица) и далее не позднее десяти календарных дней с момента изменения ранее представленных сведений;

4.3. копии аттестата соответствия системы защиты информации информационной системы требованиям по защите информации, технического отчета и протокола испытаний. В случае если мероприятия, предусмотренные в абзацах втором–десятом части первой пункта 8 Положения о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденного приказом, утверждающим настоящее Положение, не проводились, вместо копий технического отчета и протокола испытаний представляется копия договора на выполнение (оказание) соответствующих работ (услуг), заключенного с организацией, имеющей лицензию на осуществление деятельности по технической и (или) криптографической защите информации.

Сведения, предусмотренные в части первой настоящего подпункта, представляются не позднее десяти календарных дней со дня оформления (получения) аттестата соответствия системы защиты информации информационной системы требованиям по защите информации и далее не позднее десяти календарных дней с момента изменения ранее представленных сведений;

4.4. сведения о событиях информационной безопасности, в том числе о фактах нарушения или прекращения функционирования информационной системы, нарушения конфиденциальности, целостности, подлинности, доступности и сохранности информации.

Сведения, предусмотренные в части первой настоящего подпункта, представляются в произвольной форме в течение суток с момента выявления (обнаружения) соответствующих фактов.

5. Сведения, предусмотренные:

в подпунктах 4.1 и 4.2 пункта 4 настоящего Положения, – представляются посредством получения электронных услуг общегосударственной автоматизированной информационной системы с использованием личных электронных кабинетов;

в подпункте 4.3 пункта 4 настоящего Положения, – представляются посредством получения электронных услуг общегосударственной автоматизированной информационной системы с использованием личных электронных кабинетов или системы межведомственного электронного документооборота государственных органов Республики Беларусь.

6. Сведения, относящиеся к информации, распространение и (или) предоставление которой ограничено, представляются в ОАЦ с учетом установленного законодательством порядка передачи (предоставления) такой информации.

Приложение
к Положению о порядке представления
в Оперативно-аналитический центр
при Президенте Республики Беларусь
сведений о событиях информационной
безопасности, состоянии технической
и криптографической защиты информации
(в редакции приказа
Оперативно-аналитического центра
при Президенте Республики Беларусь
10.12.2024 № 259)

Форма

_____
(наименование владельца критически важного объекта информатизации)

Для служебного пользования
Экз. №

УТВЕРЖДАЮ
_____
(наименование должности
_____
руководителя организации)
_____
(подпись, инициалы, фамилия)
__.__.20___

ФОРМУЛЯР КРИТИЧЕСКИ ВАЖНОГО ОБЪЕКТА ИНФОРМАТИЗАЦИИ

_____
(наименование критически важного объекта информатизации)

1. Общие сведения о критически важном объекте информатизации:

наименование критически важного объекта информатизации;

место нахождения критически важного объекта информатизации;

критерий (критерии) отнесения объекта информатизации к критически важным объектам информатизации;

показатель (показатели) уровня вероятного ущерба национальным интересам Республики Беларусь;

подразделение (должностное лицо), ответственное за проведение работ по технической и криптографической защите информации, обрабатываемой на критически важном объекте информатизации;

сведения о вводе объекта информатизации в эксплуатацию.

2. Сведения об оборудовании и программном обеспечении, входящем в состав активов критически важного объекта информатизации:

№ п/п	Тип (вид)	Наименование, заводской (инвентарный) номер	Текущая версия программного обеспечения (сертификат соответствия)	Дата ввода в эксплуатацию	Ответственные лица
1	Программно-аппаратные средства и физические устройства				

2	Программное обеспечение (прикладное и системное)				
3	Средства защиты информации				
4	Информационные системы и информационные сети				
5	Средства обработки информации (потоков информации), средства коммуникации				
6	Средства администрирования и конфигурирования				

3. Схема расположения критически важного объекта информатизации (с указанием конкретного здания, сооружения, помещения, этажа и др.).

4. Структурная схема критически важного объекта информатизации (с указанием расположения физических устройств с номерами портов, а также физических линий связи, соединяющих физические интерфейсы технических, программно-аппаратных средств обработки информации, средств защиты информации, автоматизированного рабочего места администратора (оператора).

5. Логическая схема критически важного объекта информатизации (с указанием информационных систем, направления потоков данных, а также спецификации используемых технологий и протоколов, списков виртуальных локальных вычислительных сетей (VLAN), IP-адресов устройств).

6. Схема администрирования критически важного объекта информатизации.

УТВЕРЖДЕНО

Приказ
Оперативно-аналитического
центра при Президенте
Республики Беларусь
20.02.2020 № 66

ПОЛОЖЕНИЕ
о порядке ведения Государственного реестра критически важных объектов информатизации

1. В настоящем Положении в соответствии с пунктом 4 Положения о порядке отнесения объектов информатизации к критически важным объектам информатизации определяется порядок ведения Государственного реестра критически важных объектов информатизации (далее – реестр), в том числе включения объектов информатизации в реестр и исключения их из реестра, а также порядок предоставления сведений из реестра.

2. Для целей настоящего Положения термины используются в значениях, определенных в Положении о технической и криптографической защите информации и Положении о порядке отнесения объектов информатизации к критически важным объектам информатизации.

3. Реестр создается в целях накопления и хранения систематизированной информации о критически важных объектах информатизации, расположенных на территории Республики Беларусь, координации деятельности государственных органов и иных организаций по технической и криптографической защите информации, обрабатываемой на таких объектах.

4. Оперативно-аналитический центр при Президенте Республики Беларусь (далее – ОАЦ) осуществляет ведение реестра и обеспечивает:

накопление и хранение в реестре систематизированной информации о зарегистрированных критически важных объектах информатизации и их владельцах;

защиту информации, содержащейся в реестре;

предоставление в порядке, установленном настоящим Положением, информации о критически важных объектах информатизации, включенных в реестр.

5. Реестр включает в себя следующие сведения:

наименование критически важного объекта информатизации;

дату включения критически важного объекта информатизации в реестр;

владельца критически важного объекта информатизации (полное наименование, место нахождения, регистрационный номер в Едином государственном регистре юридических лиц и индивидуальных предпринимателей);

место нахождения критически важного объекта информатизации;

фамилию, собственное имя, отчество (если таковое имеется), должность, контактный номер телефона уполномоченного должностного лица (руководителя подразделения защиты информации), назначенного ответственным за проведение работ по технической и криптографической защите информации, обрабатываемой на критически важном объекте информатизации, а также фамилию, собственное имя, отчество (если таковое имеется), должность, контактный номер телефона лица, замещающего на время его отсутствия;

наименование государственного органа, принявшего решение об отнесении объекта информатизации к критически важным объектам информатизации, фамилию, собственное имя, отчество (если таковое имеется), должность, контактный номер телефона лица, ответственного за оперативное сопровождение данных вопросов в государственном органе;

реквизиты (дата и номер) приказа (распоряжения) руководителя государственного органа или его уполномоченного заместителя об отнесении объекта информатизации к критически важным объектам информатизации, объединении двух и более критически

важных объектов информатизации в один критически важный объект информатизации, исключении критически важного объекта информатизации из реестра;

основания для включения объекта информатизации в реестр (критерий (критерии) отнесения объекта информатизации к критически важным и показатель (показатели) уровня вероятного ущерба национальным интересам Республики Беларусь) и исключения критически важного объекта информатизации из реестра;

реквизиты (дата и номер) акта аудита системы информационной безопасности критически важного объекта информатизации, акта проверки технической и криптографической защиты информации на критически важном объекте информатизации.

6. Включение объекта информатизации в реестр осуществляется на основании решения государственного органа об отнесении объекта информатизации к критически важным объектам информатизации.

7. В течение пяти рабочих дней со дня получения копии приказа (распоряжения) руководителя государственного органа или его уполномоченного заместителя об отнесении объекта информатизации к критически важным объектам информатизации ОАЦ вносит в реестр сведения об объекте информатизации.

При отсутствии в приказе (распоряжении) всех сведений о критически важном объекте информатизации, предусмотренных в абзацах втором, четвертом–девятом пункта 5 настоящего Положения, эти сведения указываются в сопроводительном письме в адрес ОАЦ о направлении копии данного приказа (распоряжения).

8. В случае изменения сведений о критически важном объекте информатизации, предусмотренных в абзацах втором, четвертом–девятом пункта 5 настоящего Положения, государственный орган в течение десяти рабочих дней со дня изменения таких сведений информирует об этом ОАЦ для внесения соответствующих изменений в реестр. В течение трех рабочих дней со дня получения необходимых сведений ОАЦ вносит соответствующие изменения в реестр.

9. Исключение критически важного объекта информатизации из реестра осуществляется на основании решения государственного органа об исключении объекта информатизации из числа критически важных объектов информатизации после письменного согласования данного вопроса с ОАЦ.

10. В течение пяти рабочих дней со дня получения копии приказа (распоряжения) руководителя государственного органа или его уполномоченного заместителя об исключении объекта информатизации из числа критически важных объектов информатизации ОАЦ исключает этот объект информатизации из реестра путем проставления в реестре соответствующей отметки об исключении.

11. В течение пяти рабочих дней со дня получения копии приказа (распоряжения) руководителя государственного органа или его уполномоченного заместителя об объединении двух и более критически важных объектов информатизации ОАЦ актуализирует сведения, содержащиеся в реестре, путем проставления соответствующей отметки об объединении.

12. Копии приказа (распоряжения) об отнесении объекта информатизации к критически важным объектам информатизации, об исключении объекта информатизации из числа критически важных объектов информатизации, об объединении двух и более критически важных объектов информатизации в один критически важный объект информатизации, а также информация об изменении сведений о критически важном объекте информатизации направляется в ОАЦ с сопроводительным письмом посредством автоматизированной системы государственной защищенной электронной почты для обмена информацией, распространение и (или) предоставление которой ограничено, за исключением сведений, составляющих государственные секреты.

13. Сведения о критически важных объектах информатизации, содержащиеся в реестре, предоставляются государственным органам и иным организациям в объеме, необходимом для выполнения возложенных на них законодательством задач и функций, в письменной форме или форме электронного документа.

Сведения из реестра предоставляются в виде выписок из реестра, содержащих запрашиваемые сведения, в течение десяти рабочих дней со дня получения обращения. В обращении должны быть указаны:

информация о заявителе (полное наименование, место нахождения, регистрационный номер в Едином государственном регистре юридических лиц и индивидуальных предпринимателей, контактное лицо заявителя и его номер телефона);

основание для получения сведений (ссылка на акт законодательства, являющийся основанием для доступа к сведениям, находящимся в реестре);

запрашиваемые сведения.

В случае отсутствия запрашиваемых сведений или невозможности их предоставления ОАЦ сообщает об этом заявителю в письменном виде в течение десяти рабочих дней с момента получения обращения.

УТВЕРЖДЕНО

Приказ
Оперативно-аналитического
центра при Президенте
Республики Беларусь
29.07.2013 № 48
(в редакции приказа
Оперативно-аналитического
центра при Президенте
Республики Беларусь
20.02.2020 № 66)

ИНСТРУКЦИЯ
о порядке осуществления контроля за технической защитой государственных секретов

1. В настоящей Инструкции в соответствии с Законом Республики Беларусь «О государственных секретах» и иным законодательством о государственных секретах устанавливается порядок осуществления контроля за технической защитой государственных секретов (далее – контроль) в государственных органах и иных организациях, осуществляющих деятельность с использованием государственных секретов, за исключением контроля в деятельности органов государственной безопасности (далее – организации).

2. Для целей настоящей Инструкции термины используются в значениях, определенных в Законе Республики Беларусь «О государственных секретах», а также следующие термины и их определения:

аттестация объекта информатизации – комплекс организационно-технических мероприятий, осуществляемых до ввода объекта информатизации в эксплуатацию, в результате которых документально подтверждается соответствие объекта информатизации требованиям законодательства о государственных секретах;

объект информатизации – средство вычислительной техники, предназначенное для обработки информации, содержащей государственные секреты, или помещение, предназначенное для проведения мероприятий, в ходе которых циркулирует речевая информация, содержащая государственные секреты.

3. Контроль проводится в целях проверки выполнения организациями требований законодательства о государственных секретах, а также оценки обоснованности, достаточности и эффективности принятых ими мер по технической защите государственных секретов.

4. Контроль осуществляется Оперативно-аналитическим центром при Президенте Республики Беларусь (далее – ОАЦ) в форме проверок, проводимых в соответствии с планом проверок технической защиты государственных секретов, 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 при наличии сведений, в том числе полученных от государственного органа, иной организации или физического лица, свидетельствующих о нарушении требований законодательства о государственных секретах или о фактах возникновения предпосылок к несанкционированному распространению информации, содержащей государственные секреты.

5. Для проведения проверки решением начальника ОАЦ назначается комиссия и определяется ее председатель.

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.

6. Для проведения проверки на каждого члена комиссии в соответствии с законодательством о государственных секретах оформляется предписание, которое подписывается начальником ОАЦ и заверяется гербовой печатью ОАЦ.

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

8. При проведении проверки каждый член комиссии должен иметь предписание и служебное удостоверение сотрудника ОАЦ.

9. Проверка начинается с внесения предписаний и представления комиссии руководителю организации или его уполномоченному заместителю.

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

10. Проверочные мероприятия проводятся в присутствии определенных руководителем организации или его уполномоченным заместителем сотрудников подразделения по защите государственных секретов, подразделения технической защиты информации или иного подразделения (должностных лиц), ответственного за обеспечение технической защиты государственных секретов.

11. В ходе проверки оцениваются:

наличие подразделения технической защиты информации или иного подразделения (должностных лиц), ответственного за обеспечение технической защиты государственных секретов, их задачи и функции с учетом требований законодательства о государственных секретах;

наличие и содержание перечня объектов информатизации;

содержание локальных правовых актов, регламентирующих вопросы обеспечения технической защиты государственных секретов в организации;

наличие иных документов, определяющих порядок и результаты проведения мероприятий по созданию систем защиты информации на объектах информатизации, аттестации этих объектов информатизации и вводу их в эксплуатацию, соответствие содержания данных документов и результатов проведения мероприятий требованиям законодательства о государственных секретах;

реализация непосредственно на объектах информатизации (в реальных условиях эксплуатации) мер технической защиты государственных секретов в соответствии с требованиями законодательства о государственных секретах, их эффективность и достаточность.

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

13. Срок проведения проверки не может превышать:

тридцати рабочих дней – для проверок, указанных в части первой пункта 4 настоящей Инструкции;

десяти рабочих дней – для проверок, указанных в части второй пункта 4 настоящей Инструкции.

При наличии значительного объема документов и (или) количества объектов информатизации, подлежащих проверке, срок проведения проверки по решению начальника ОАЦ может быть однократно продлен не более чем на пятнадцать рабочих дней.

14. По результатам проверки комиссией составляется акт проверки в количестве экземпляров, предусмотренных настоящей Инструкцией, с отражением в этом акте экспертной оценки обеспечения технической защиты государственных секретов, выявленных нарушений и недостатков, а также предложений по их устранению.

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

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

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

Первый экземпляр акта проверки в течение трех рабочих дней после его доведения до сведения руководителя организации или его уполномоченного заместителя в установленном порядке направляется в данную организацию, второй – остается в ОАЦ. Третий и четвертый экземпляры акта, как правило, направляются в вышестоящую по отношению к проверяемой организацию (при ее наличии) и в организацию, являющуюся владельцем государственных секретов, деятельность с использованием которых она осуществляет (если организация не наделена полномочием по отнесению сведений к государственным секретам).

15. 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 обоснованности указанных доводов может быть назначена специальная комиссия. Результаты рассмотрения обоснованности доводов отражаются в письменном заключении, которое направляется в организацию.

16. В случае обнаружения в ходе проверки нарушений требований законодательства о государственных секретах, создающих угрозу национальной безопасности, начальник ОАЦ или его уполномоченный заместитель выносит письменное требование (предписание) об устранении выявленных нарушений и (или) приостановлении проведения на объектах информатизации работ, в ходе которых обрабатывается (циркулирует) информация, содержащая государственные секреты.

Письменное требование (предписание), а также информация о выявленных нарушениях, послуживших основанием для его вынесения, доводится до сведения руководителя организации, в которой выявлены нарушения, или его уполномоченного заместителя. Руководитель организации или его уполномоченный заместитель обязан принять меры по приостановлению проведения на объектах информатизации работ, в ходе которых обрабатывается (циркулирует) информация, содержащая государственные секреты, до устранения выявленных нарушений.

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

Решение о возобновлении проведения на объектах информатизации работ, в ходе которых обрабатывается (циркулирует) информация, содержащая государственные секреты, принимается начальником ОАЦ или его уполномоченным заместителем при условии устранения нарушений, послуживших основанием вынесения письменного требования (предписания). Для подтверждения устранения указанных нарушений организация предоставляет в ОАЦ необходимые документы, а также возможность удостовериться в этом на месте.

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.

17. Вынесенные по результатам проверки решения по акту проверки, письменное требование (предписание) об устранении нарушений и (или) приостановлении проведения на объектах информатизации работ, в ходе которых обрабатывается (циркулирует) информация, содержащая государственные секреты, а также действия (бездействие) членов комиссии могут быть обжалованы организацией в суд в порядке, установленном законодательными актами.

Приложение 1
к Положению о порядке проведения
государственной экспертизы средств
технической и криптографической
защиты информации
(в редакции приказа
Оперативно-аналитического
центра при Президенте
Республики Беларусь
20.02.2020 № 66)

Форма

ЗАЯВКА
на проведение государственной экспертизы продукции

1. _____
(наименование (фамилия, имя, отчество (если таковое имеется) заявителя)
место нахождения (место жительства) _____
банковские реквизиты _____
УНП _____, телефон _____, факс _____
заявляет, что _____,
(наименование продукции, код ОКРБ 007-2012, код ТН ВЭД)
изготовленная _____
(наименование, место нахождения изготовителя)
товаросопроводительный документ _____
(реквизиты документа и объем партии)
по _____,
(обозначение и наименование документации изготовителя)
соответствует требованиям _____
(обозначение и наименование документов)
и просит провести государственную экспертизу данной продукции на соответствие требованиям указанных документов.

2. Обязуемся:

выполнять все условия проведения государственной экспертизы;

оплатить все расходы по проведению государственной экспертизы;

обеспечивать соответствие продукции, прошедшей государственную экспертизу, требованиям по технической и криптографической защите информации, указанным в экспертном заключении.

Приложение:

Руководитель организации
(индивидуальный предприниматель) _____ _____
(подпись) (инициалы, фамилия)

___ _____ 20__ г.

Приложение 2
к Положению о порядке проведения
государственной экспертизы средств
технической и криптографической
защиты информации
(в редакции приказа
Оперативно-аналитического
центра при Президенте
Республики Беларусь
20.02.2020 № 66)

Форма

АКТ
отбора образцов продукции

от ___ _____ 20__ г.

На _____
(местонахождение продукции, наименование
_____ мною,
(фамилия, имя, отчество (если таковое имеется) заявителя)
_____,
(фамилия, имя, отчество (если таковое имеется) эксперта органа государственной экспертизы)
в присутствии _____
(фамилия, имя, отчество (если таковое имеется) представителя заявителя)
отобраны образцы _____,
(наименование продукции, код ОКРБ 007-2012)
изготовленной _____,
(наименование изготовителя)
для оценки соответствия требованиям _____
(наименование и обозначение документов)
Отбор образцов произведен в соответствии с _____
(наименование и обозначение документов)
_____

№ п/п	Наименование образцов продукции, ее реквизиты (изготовитель, штриховой код, хэш-значение и др.)	Единица измерения	Размер партии	Дата изготовления (конечный срок реализации, номер изделия и т.п.)	Количество отобранных образцов

Результаты внешнего осмотра _____
Информация об идентификации продукции _____
Упаковка _____
Условия и место хранения _____

Эксперт _____ _____
(подпись) (инициалы, фамилия)

Представитель заявителя _____ _____
(подпись) (инициалы, фамилия)

Приложение 1
к Инструкции о порядке проведения
аккредитации поставщиков услуг
в Государственной системе
управления открытыми ключами
проверки электронной цифровой
подписи Республики Беларусь
и осуществления контроля
за соблюдением условий аккредитации
(в редакции приказа
Оперативно-аналитического
центра при Президенте
Республики Беларусь
20.02.2020 № 66)

ПЕРЕЧЕНЬ
условий, на соответствие которым осуществляется аккредитация поставщиков услуг в ГосСУОК

1. Поставщики услуг в ГосСУОК должны иметь специальное разрешение (лицензию) на деятельность по технической и (или) криптографической защите информации в части составляющих данный вид деятельности работ и (или) услуг по:

удостоверению формы внешнего представления электронного документа на бумажном носителе и распространению открытых ключей проверки электронной цифровой подписи (для аккредитации в качестве УЦ);

распространению открытых ключей проверки электронной цифровой подписи (для аккредитации в качестве РЦ).

2. Аккредитация УЦ в ГосСУОК осуществляется на соответствие следующим условиям:

2.1. УЦ должен разработать политику применения сертификатов УЦ и регламент УЦ;

2.2. в политике применения сертификатов УЦ должны быть определены требования:

по управлению ключами (по выработке личного ключа подписи УЦ, хранению, резервному копированию и восстановлению личного ключа подписи УЦ, распространению открытых ключей УЦ, использованию личного ключа УЦ, действиям по окончании срока действия личного ключа УЦ, управлению средствами электронной цифровой подписи), используемыми для издания сертификатов открытых ключей;

по управлению сертификатами открытых ключей (по регистрации субъектов для получения сертификата открытого ключа, изданию, возобновлению действия и обновлению данных, распространению, отзыву и приостановке действия сертификатов открытых ключей), издаваемыми УЦ;

по организации функционирования и управления деятельностью УЦ;

2.3. для реализации услуг УЦ и обеспечения своей деятельности поставщики услуг, кроме выполнения требований по управлению деятельностью УЦ, определенных в политике применения сертификатов УЦ, должны использовать в УЦ следующие программные, программно-аппаратные и технические средства:

2.3.1. системное и прикладное программное обеспечение. При этом:

входящие в состав системного и прикладного программного обеспечения операционные системы, системы управления базами данных, программное обеспечение архивного хранения, программное обеспечение резервного копирования и при необходимости другое программное обеспечение должны быть приобретены в соответствии с законодательством (на основании лицензионного договора или быть свободно распространяемыми);

системное и прикладное программное обеспечение должно быть установлено, сконфигурировано и находиться в работоспособном состоянии;

2.3.2. средства УЦ, имеющие сертификат соответствия Национальной системы подтверждения соответствия Республики Беларусь требованиям технического регламента

Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY). При этом:

указанные средства должны использовать аппаратный датчик случайных чисел (для генерации случайных чисел), а также обеспечивать невозможность доступа к криптографическим ключам в случае несанкционированного вскрытия корпуса;

настройка и выполнение функций указанных средств должны осуществляться путем подачи команд с автоматизированного рабочего места администратора этих средств. Взаимодействие средств УЦ с автоматизированным рабочим местом администратора должно осуществляться по надежному каналу передачи данных, который логически отличается от других информационных каналов и обеспечивает гарантированную идентификацию конечных сторон, а также защиту данных от модификации и раскрытия. Средства канального (линейного) шифрования между средствами УЦ и автоматизированным рабочим местом администратора должны иметь сертификат соответствия Национальной системы подтверждения соответствия Республики Беларусь требованиям технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY);

2.3.3. средства канального (линейного) шифрования между УЦ и удаленным РЦ, имеющие сертификат соответствия Национальной системы подтверждения соответствия Республики Беларусь требованиям технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY);

2.3.4. технические средства обеспечения функционирования УЦ. При этом технические средства обеспечения работы программного комплекса УЦ должны быть исправны, корректно сконфигурированы, работоспособны и включать:

сервер (серверы) УЦ;

средства резервного копирования;

сервер (устройство) получения точного времени;

телекоммуникационное оборудование;

электронные вычислительные машины рабочих мест сотрудников УЦ;

устройства печати на бумажных носителях (принтеры).

При реализации УЦ услуги по регистрации субъектов должны быть дополнительно предусмотрены следующие технические средства:

сервер (серверы) или автоматизированное рабочее место РЦ;

устройства печати на бумажных носителях (принтеры);

средства обеспечения бесперебойной работы;

устройства подтверждения подлинности идентификационных документов.

Технические средства должны обеспечивать возможность непрерывной и бесперебойной работы программного обеспечения УЦ, а также производительность (скорость выполнения операций), достаточную для выполнения оператором любой прикладной задачи (услуги УЦ) в течение 30 минут;

2.4. система защиты информации информационной системы УЦ должна быть создана и аттестована по классам 3-юл и 3-фл типовых информационных систем в порядке, установленном законодательством;

2.5. требования по обеспечению безопасности при монтаже, наладке, эксплуатации и обслуживании технических средств УЦ (защита от воздействий электрического тока, электромагнитных полей, акустических шумов и тому подобное) по допустимым уровням освещенности, вибрационных и шумовых нагрузок должны быть согласованы с требованиями документации на соответствующие виды оборудования;

2.6. серверы УЦ, серверы баз данных, серверы средств резервного копирования и телекоммуникационное оборудование поставщиков услуг должны размещаться в выделенном помещении;

2.7. требования по физическому доступу к компонентам УЦ:

физический доступ к компонентам УЦ должен быть защищен как минимум двумя уровнями доступа;

на каждом уровне доступа должна осуществляться проверка разрешения на доступ;

контроль доступа к программным компонентам УЦ должен осуществляться с использованием двухфакторной аутентификации, включая использование аппаратных носителей ключевой информации;

серверное и рабочие помещения УЦ должны быть оборудованы системами контроля доступа и видеонаблюдения;

охрана объекта, в котором размещены технические средства УЦ, должна быть обеспечена в соответствии с Указом Президента Республики Беларусь от 25 октября 2007 г. № 534 «О мерах по совершенствованию охранной деятельности»;

2.8. требования к электроснабжению:

технические средства УЦ в повседневном режиме должны быть подключены к электрической сети энергоснабжающей организации;

электрические сети и электрооборудование, используемые в УЦ, должны соответствовать требованиям законодательства, в том числе обязательным для соблюдения требованиям технических нормативных правовых актов;

серверы, телекоммуникационное оборудование и технические средства сотрудников УЦ должны быть подключены к источникам бесперебойного питания, обеспечивающим их работу в течение 30 минут после прекращения основного электроснабжения;

в случае прекращения подачи электрической энергии должно быть предусмотрено резервное электропитание технических средств УЦ;

источник резервного электропитания должен быть подключен к потребителям электропитания и обеспечивать автоматическую подачу необходимой электрической энергии в течение 30 минут после прекращения подачи электрической энергии от энергоснабжающей организации (источник резервного электропитания не требуется при наличии двух вводов в здание УЦ от различных подстанций);

2.9. серверное помещение УЦ должно быть оборудовано двумя установками кондиционирования воздуха. Данные установки должны управляться автоматизированной системой и обеспечивать постоянный температурно-влажностный режим, определенный эксплуатационной документацией на технические средства УЦ;

2.10. серверное помещение УЦ должно быть оборудовано системами пожарной сигнализации, автоматического газопожаротушения, газоудаления и противопожарной дверью с огнестойкостью не менее одного часа;

2.11. пожарная безопасность помещений УЦ должна обеспечиваться в соответствии с требованиями законодательства, в том числе обязательными для соблюдения требованиями технических нормативных правовых актов.

3. Аккредитация РЦ в ГосСУОК осуществляется на соответствие следующим условиям:

3.1. РЦ должен присоединиться к соответствующей политике применения сертификатов УЦ и выполнять ее в части оказания услуг по регистрации субъектов УЦ;

3.2. для реализации услуг РЦ и обеспечения своей деятельности, кроме выполнения требований по управлению деятельностью РЦ, определенных в политике применения сертификатов УЦ, в РЦ должны использоваться следующие программные, программно-аппаратные и технические средства:

3.2.1. системное и прикладное программное обеспечение. При этом:

входящие в состав системного и прикладного программного обеспечения операционные системы, системы управления базами данных, программное обеспечение архивного хранения, программное обеспечение резервного копирования и при необходимости другое программное обеспечение должны быть приобретены в соответствии с законодательством (на основании лицензионного договора или быть свободно распространяемыми);

системное и прикладное программное обеспечение должно быть установлено, сконфигурировано и находиться в работоспособном состоянии;

3.2.2. средства РЦ, имеющие сертификат соответствия Национальной системы подтверждения соответствия Республики Беларусь требованиям технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY);

3.2.3. средства канального (линейного) шифрования между удаленным РЦ и УЦ, имеющие сертификат соответствия Национальной системы подтверждения соответствия Республики Беларусь требованиям технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY);

3.2.4. технические средства обеспечения функционирования РЦ. При этом технические средства обеспечения работы программного комплекса РЦ должны быть исправны, корректно сконфигурированы, работоспособны и включать:

электронные вычислительные машины рабочих мест сотрудников РЦ;

устройства печати на бумажных носителях (принтеры);

устройства подтверждения подлинности идентификационных документов (за исключением РЦ, реализующих функции по достоверному подтверждению полномочий, предоставленных физическому лицу от имени организации или другого физического лица);

телекоммуникационное оборудование;

средства обеспечения бесперебойной работы.

Технические средства обеспечения программного комплекса РЦ могут включать серверы баз данных и (или) серверы архивного хранения электронных документов.

Технические средства должны обеспечивать производительность (скорость выполнения операций), достаточную для выполнения оператором любой прикладной задачи (услуги РЦ), а также непрерывную и бесперебойную работу в ходе выполнения этой прикладной задачи.

Программные, программно-аппаратные и технические средства РЦ должны быть протестированы на предмет корректного взаимодействия с УЦ, в интересах которого РЦ будут оказываться услуги;

3.3. система защиты информации информационной системы РЦ должна быть создана и аттестована по классам 3-юл и 3-фл типовых информационных систем в порядке, установленном законодательством;

3.4. требования по обеспечению безопасности при монтаже, наладке, эксплуатации и обслуживании технических средств РЦ (защита от воздействий электрического тока, электромагнитных полей, акустических шумов и тому подобное) по допустимым уровням освещенности, вибрационных и шумовых нагрузок должны соответствовать документации на соответствующие виды оборудования;

3.5. электронные вычислительные машины рабочих мест сотрудников РЦ и телекоммуникационное оборудование РЦ должны размещаться в выделенном помещении. В случае невозможности выделения такого помещения, а также организации дополнительных переносных рабочих мест сотрудников РЦ для реализации его функций при выезде к заявителю должна обеспечиваться защита технических средств от несанкционированного изменения их конфигурации и несанкционированного доступа к интерфейсным портам этих средств. В таких случаях должно быть обеспечено применение программных, программно-аппаратных средств защиты от несанкционированного доступа, саморазрушающихся наклеек, стикеров, а также хранение технических средств в опечатываемых коммутационных шкафах;

3.6. требования по физическому доступу к компонентам РЦ:

физический доступ к компонентам РЦ должен быть защищен как минимум двумя уровнями доступа;

на каждом уровне доступа должна осуществляться проверка разрешения на доступ;

контроль доступа к программным компонентам РЦ должен осуществляться с использованием двухфакторной аутентификации, включая использование аппаратных носителей ключевой информации;

рабочие места РЦ, как правило, должны быть оборудованы системами видеонаблюдения;

охрана объекта, в котором размещены технические средства РЦ, должна быть обеспечена в соответствии с Указом Президента Республики Беларусь от 25 октября 2007 г. № 534;

3.7. требования по электроснабжению:

технические средства РЦ в повседневном режиме должны быть подключены к электрической сети энергоснабжающей организации;

электрические сети и электрооборудование, используемые в РЦ, должны соответствовать требованиям законодательства, в том числе обязательным для соблюдения требованиям технических нормативных правовых актов;

телекоммуникационное оборудование и технические средства сотрудников РЦ должны быть подключены к источникам бесперебойного питания, обеспечивающим их работу в течение времени, достаточного для выполнения оператором любой прикладной задачи (услуги РЦ);

3.8. пожарная безопасность помещений РЦ должна обеспечиваться в соответствии с требованиями законодательства, в том числе обязательными для соблюдения требованиями технических нормативных правовых актов.

Приложение 3
к Инструкции о порядке проведения
аккредитации поставщиков услуг
в Государственной системе
управления открытыми ключами
проверки электронной цифровой
подписи Республики Беларусь
и осуществления контроля
за соблюдением условий аккредитации
(в редакции приказа
Оперативно-аналитического
центра при Президенте
Республики Беларусь
20.02.2020 № 66)

ПЕРЕЧЕНЬ
документов, представляемых поставщиком услуг при аккредитации в ГосСУОК

1. Копии учредительного документа, положения о структурном подразделении, которое будет выполнять функции поставщика услуг, свидетельства о государственной регистрации в Едином государственном регистре юридических лиц и индивидуальных предпринимателей.

2. Для аккредитации в качестве УЦ заявитель, кроме документов, перечисленных в пункте 1 настоящего приложения, представляет:

документ с указанием сведений о реквизитах сертификатов соответствия Национальной системы подтверждения соответствия Республики Беларусь в отношении используемых средств УЦ, средств канального (линейного) шифрования;

копию аттестата соответствия требованиям по защите информации системы защиты информации информационной системы УЦ, выданного в соответствии с законодательством, а также копию технического задания на создание системы защиты информации данной информационной системы либо сведения о представлении указанного технического задания в орган по аккредитации;

документы, взаимосвязанные с политикой применения сертификатов и регламентом УЦ (стандарты организации, документированные процедуры, рабочие инструкции), либо их копии;

документы, содержащие информацию об инфраструктуре поставщика услуг (здания, помещения, оборудование, технические средства и другое) и о компетентности персонала (список сотрудников, копии документов о высшем образовании либо высшем или профессионально-техническом образовании и переподготовке или повышении квалификации в области защиты информации);

документы, содержащие информацию об обеспечении пожарной безопасности, охраны и контроля доступа в помещения УЦ, обеспечении гарантированным непрерывным электроснабжением технических средств УЦ.

3. Для аккредитации в качестве РЦ заявитель, кроме документов, перечисленных в пункте 1 настоящего приложения, представляет:

копию регламента работы РЦ заявителя;

документ с указанием сведений о реквизитах сертификатов соответствия Национальной системы подтверждения соответствия Республики Беларусь в отношении используемых средств РЦ, средств канального (линейного) шифрования;

копию аттестата соответствия требованиям по защите информации системы защиты информации информационной системы РЦ, выданного в соответствии с законодательством, а также копию технического задания на создание системы защиты информации данной информационной системы либо сведения о представлении указанного технического задания в орган по аккредитации;

документы (акты либо протоколы тестирования, утвержденные руководителями организаций), подтверждающие положительные результаты тестирования программных, программно-аппаратных и технических средств РЦ на предмет корректного взаимодействия с УЦ;

документы, взаимосвязанные с политикой (политиками) применения сертификатов УЦ, к которой (которым) присоединяется РЦ, и с регламентом работы РЦ (стандарты организации, документированные процедуры, рабочие инструкции), либо их копии;

документы, содержащие информацию об инфраструктуре поставщика услуг (здания, помещения, оборудование, технические средства и другое) и о компетентности персонала (список сотрудников, копии документов о высшем образовании либо высшем или профессионально-техническом образовании и переподготовке или повышении квалификации в области защиты информации);

документы, содержащие информацию об обеспечении пожарной безопасности, охраны и контроля доступа в помещения РЦ, обеспечении гарантированным непрерывным электроснабжением технических средств РЦ.