ПРИКАЗ ОПЕРАТИВНО-АНАЛИТИЧЕСКОГО ЦЕНТРА ПРИ ПРЕЗИДЕНТЕ РЕСПУБЛИКИ БЕЛАРУСЬ
10 декабря 2024 г. № 259

Об изменении приказов Оперативно-аналитического центра при Президенте Республики Беларусь от 28 марта 2014 г. № 26 и от 20 февраля 2020 г. № 66

На основании пункта 4 статьи 33 Закона Республики Беларусь от 17 июля 2018 г. № 130-З «О нормативных правовых актах», подпункта 6.4 пункта 6, подпунктов 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, ПРИКАЗЫВАЮ:

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

1.1. из абзаца третьего пункта 2 Положения о порядке размещения программно-технических средств, информационных систем (ресурсов) государственных организаций на ресурсах республиканского центра обработки данных и (или) республиканской платформы, утвержденного приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 28 марта 2014 г. № 26, слово «совместное» исключить;

1.2. в приказе Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449»:

пункт 4 исключить;

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

Положение о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденное этим приказом, изложить в новой редакции (прилагается);

Положение о порядке представления в Оперативно-аналитический центр при Президенте Республики Беларусь сведений о событиях информационной безопасности, состоянии технической и криптографической защиты информации, утвержденное этим приказом, изложить в новой редакции (прилагается).

2. Проектирование, создание и (или) аттестация систем защиты информации информационных систем, осуществляемые на основании договоров, заключенных до вступления в силу настоящего приказа, но не исполненных на дату вступления его в силу:

осуществляются в соответствии с законодательством, действовавшим на дату заключения указанных договоров;

по решению собственников (владельцев) информационных систем могут осуществляться в соответствии с настоящим приказом, если иное не предусмотрено законодательными актами.

3. Настоящий приказ вступает в силу в следующем порядке:

подпункт 1.2 пункта 1 и пункт 2 – с 1 марта 2025 г.;

иные положения настоящего приказа – после его официального опубликования.

Начальник **А.Ю.Павлюченко**

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
(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.