ПРИКАЗ ОПЕРАТИВНО-АНАЛИТИЧЕСКОГО ЦЕНТРА ПРИ ПРЕЗИДЕНТЕ РЕСПУБЛИКИ БЕЛАРУСЬ
12 ноября 2021 г. № 195

О технической и криптографической защите персональных данных

На основании подпункта 6.4 пункта 6 Положения о технической и криптографической защите информации, утвержденного Указом Президента Республики Беларусь от 16 апреля 2013 г. № 196, и абзаца шестого пункта 3 статьи 17 Закона Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных» ПРИКАЗЫВАЮ:

1. Установить, что техническая и криптографическая защита персональных данных осуществляется в соответствии с Положением о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, Положением о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденными приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66. При этом операторы (уполномоченные лица) обеспечивают выполнение требований, установленных для собственников (владельцев) информационных систем, в которых обрабатываются персональные данные.

2. Внести в приказ 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» следующие изменения:

2.1. в Положении о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденном этим приказом:

пункт 1 дополнить частью следующего содержания:

«Требования настоящего Положения могут не применяться собственниками (владельцами) информационных систем, в которых обрабатываются только общедоступные персональные данные.»;

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, Законе Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» (за исключением термина «персональные данные»), Законе Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных», а также следующие термины и их определения:»;

из абзаца второго слово «организации» исключить;

пункт 4 дополнить частью следующего содержания:

«Физические лица, в том числе индивидуальные предприниматели, являющиеся собственниками (владельцами) информационных систем, в которых обрабатываются персональные данные, вправе выполнять работы по технической и криптографической защите этих данных самостоятельно (без создания (назначения) подразделения защиты информации или иного подразделения (должностного лица), ответственного за обеспечение защиты информации) либо с привлечением специализированной организации.»;

часть вторую пункта 7 дополнить предложением следующего содержания: «Физические лица, в том числе индивидуальные предприниматели, являющиеся собственниками (владельцами) информационных систем, в которых обрабатываются

персональные данные, составляют акт отнесения информационной системы к классу типовых информационных систем в произвольной форме.»;

абзац третий пункта 8 изложить в следующей редакции:

«издание политики информационной безопасности. При этом физическое лицо, являющееся собственником (владельцем) информационной системы, в которой обрабатываются персональные данные, за исключением индивидуального предпринимателя, вправе не издавать политику информационной безопасности;»;

в пункте 9:

из абзаца первого слово «организации» исключить;

из абзаца второго слова «в организации» исключить;

абзац третий изложить в следующей редакции:

«перечень информационных систем, отнесенных к соответствующим классам типовых информационных систем, перечень средств вычислительной техники, а также сведения о подразделении защиты информации или ином подразделении (должностном лице), ответственном за обеспечение защиты информации (если создание (назначение) такого подразделения (должностного лица) предусмотрено законодательными актами);»;

часть вторую пункта 10 после абзаца четвертого дополнить абзацами следующего содержания:

«порядок обезличивания персональных данных (в случае их обработки в информационной системе) с применением методов согласно приложению 5;

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 14 настоящего Положения;»;

пункт 12 изложить в следующей редакции:

«12. В случае документирования создания информационных систем в соответствии с техническими нормативными правовыми актами, регламентирующими порядок создания автоматизированных систем, сведения, указанные в пункте 11 настоящего Положения, могут быть предусмотрены в документах на автоматизированную информационную систему.»;

в пункте 14:

слова «мер защиты информации, реализованных в информационной системе» заменить словами «требований, реализованных в системе защиты информации информационной системы»;

дополнить пункт предложением следующего содержания: «Такие требования применяются в соответствии с договором на оказание соответствующих услуг.»;

пункт 18 изложить в следующей редакции:

«18. В случае документирования создания информационных систем в соответствии с техническими нормативными правовыми актами, регламентирующими порядок создания автоматизированных систем, сведения, указанные в пункте 17 настоящего Положения, могут быть предусмотрены в документах на автоматизированную информационную систему.»;

дополнить Положение пунктом 19^1 следующего содержания:

«19^1. 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 данных тем же собственником (владельцем) информационной системы названному физическому лицу может осуществляться без использования средств криптографической защиты информации.»;

пункт 22 дополнить словами «(если создание (назначение) такого подразделения (должностного лица) предусмотрено законодательными актами)»;

приложения 1, 3 и 4 к этому Положению изложить в новой редакции (прилагаются);

дополнить Положение приложением 5 (прилагается);

2.2. в Положении о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденном этим приказом:

пункт 1 дополнить частью следующего содержания:

«Требования настоящего Положения могут не применяться собственниками (владельцами) информационных систем, в которых обрабатываются только общедоступные персональные данные.»;

абзац первый пункта 2 изложить в следующей редакции:

«2. Для целей настоящего Положения термины используются в значениях, определенных в Положении о технической и криптографической защите информации, Законе Республики Беларусь «Об информации, информатизации и защите информации» (за исключением термина «персональные данные»), Законе Республики Беларусь «О защите персональных данных», а также следующие термины и их определения:»;

в пункте 4:

часть первую дополнить предложением следующего содержания: «Физические лица, в том числе индивидуальные предприниматели, являющиеся собственниками (владельцами) информационных систем, в которых обрабатываются персональные данные, вправе выполнять работы по аттестации единолично.»;

в части второй:

из абзаца второго слово «организации» исключить;

абзац третий после слова «отнесения» дополнить словами «информационной системы»;

часть третью дополнить словами «(если создание (назначение) такого подразделения (должностного лица) предусмотрено законодательными актами)»;

в пункте 9:

часть вторую изложить в следующей редакции:

«При аттестации информационных систем классов «3-ин», «3-спец», «3-бг», «3-юл» и «3-дсп» мероприятия, предусмотренные в абзацах седьмом и восьмом пункта 8 настоящего Положения, проводятся с использованием средства контроля эффективности защищенности информации.»;

дополнить пункт частью следующего содержания:

«Мероприятия, предусмотренные в абзацах втором–девятом пункта 8 настоящего Положения, могут не проводиться при выполнении 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.»;

в пункте 10:

часть первую изложить в следующей редакции:

«10. Программа и методика аттестации разрабатываются на основании исходных данных и должны содержать перечень выполняемых работ с указанием ответственных лиц, сроки выполнения этих работ, информацию о методах проверки требований безопасности, реализованных в системе защиты информации, перечень используемой контрольной аппаратуры и тестовых средств.»;

абзац второй части второй дополнить предложением следующего содержания: «Физические лица, в том числе индивидуальные предприниматели, являющиеся собственниками (владельцами) информационных систем, в которых обрабатываются персональные данные, вправе разработать программу и методику аттестации единолично;»;

абзац второй пункта 11 и абзац второй части первой пункта 12 после слов «(владельца) информационной системы» дополнить словами «, физическим лицом, в том

числе индивидуальным предпринимателем, являющимся собственником (владельцем) информационной системы, в которой обрабатываются персональные данные,»;

2.3. в Положении о порядке технической и криптографической защиты информации, обрабатываемой на критически важных объектах информатизации, утвержденном этим приказом:

в части второй пункта 8 слова «информационной безопасности критически важного объекта информатизации» заменить словами «технической и криптографической защиты информации»;

приложение к этому Положению изложить в новой редакции (прилагается);

2.4. в Положении о порядке представления в Оперативно-аналитический центр при Президенте Республики Беларусь сведений о событиях информационной безопасности, состоянии технической и криптографической защиты информации, утвержденном этим приказом:

пункт 1 дополнить частью следующего содержания:

«Требования настоящего Положения могут не применяться собственниками (владельцами) информационных систем, в которых обрабатываются только общедоступные персональные данные.»;

пункт 2 изложить в следующей редакции:

«2. Для целей настоящего Положения термины используются в значениях, определенных в Положении о технической и криптографической защите информации, Законе Республики Беларусь «Об информации, информатизации и защите информации» (за исключением термина «персональные данные»), Законе Республики Беларусь «О защите персональных данных».»;

из подпункта 3.4 пункта 3 слова «– не позднее чем за десять рабочих дней до запланированной даты приостановления» исключить.

3. Действие подпунктов 2.1 и 2.2 пункта 2 настоящего приказа не распространяется на:

информационные системы, предназначенные для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам (далее – 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 – аттестат соответствия);

вновь создаваемые или модернизируемые информационные системы, на которые на дату вступления в силу настоящего приказа утверждены технические задания. 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 аттестацию (обращаются за проведением аттестации) систем защиты информации информационных систем в порядке, установленном приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 (с изменениями и дополнениями, внесенными в него настоящим приказом).

Собственники (владельцы) информационных систем, указанных в части первой настоящего пункта, вправе руководствоваться приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 (с изменениями и дополнениями, внесенными в него настоящим приказом) без учета переходных положений, определенных частями первой и второй настоящего пункта.

4. Настоящий приказ вступает в силу с 15 ноября 2021 г.

Начальник **А.Ю.Павлюченко**

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
12.11.2021 № 195)

КЛАССЫ
типовых информационных систем

1. Класс 6-частн – негосударственные информационные системы, в которых обрабатывается общедоступная информация (в том числе общедоступные персональные данные) и которые не имеют подключений к открытым каналам передачи данных.

2. Класс 6-гос – государственные информационные системы, в которых обрабатывается общедоступная информация (в том числе общедоступные персональные данные) и которые не имеют подключений к открытым каналам передачи данных.

3. Класс 5-частн – негосударственные информационные системы, в которых обрабатывается общедоступная информация (в том числе общедоступные персональные данные) и которые подключены к открытым каналам передачи данных.

4. Класс 5-гос – государственные информационные системы, в которых обрабатывается общедоступная информация (в том числе общедоступные персональные данные) и которые подключены к открытым каналам передачи данных.

5. Класс 4-ин – информационные системы, в которых обрабатываются персональные данные, за исключением специальных персональных данных, и которые не имеют подключений к открытым каналам передачи данных.

6. 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.

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

8. 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.

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

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

11. 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.

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

13. 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.

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

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
12.11.2021 № 195)

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

	Наименование требований	Условие об обязательности выполнения требований в соответствии с классом 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 информации о событиях информационной безопасности, подлежащих регистрации (идентификация и аутентификация пользователей, нарушения прав доступа пользователей, выявленные нарушения информационной безопасности, информация о функционировании средств вычислительной техники, сетевого оборудования и средств защиты информации и другое)	+	+	+	+	+	+	+	+	+	+
1.2	Обеспечение сбора и хранения информации о событиях информационной безопасности в течение установленного срока хранения, но не менее одного года	+	+	+	+	+	+	+	+	+	+
1.3	Обеспечение централизованного сбора и хранения информации о событиях информационной безопасности в течение установленного срока хранения, но не менее одного года	+/–	+/–	+	+/–	+/–	+	+	+	+/–	+
1.4	Определение способа и периодичности мониторинга (просмотра, анализа) событий информационной безопасности уполномоченными на это пользователями информационной системы	+	+	+	+	+	+	+	+	+	+
1.5	Обеспечение сбора и хранения информации о функционировании средств вычислительной техники, сетевого оборудования и средств защиты информации в течение установленного срока хранения, но не менее одного года	+	+	+	+	+	+	+	+	+	+

2	Требования по обеспечению защиты данных										
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, сетевого оборудования, системного программного обеспечения и средств защиты информации	+	+	+	+	+	+	+	+	+	+
2.3	Обеспечение защиты от несанкционированного доступа к резервным копиям, параметрам настройки сетевого 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 вычислительной техники, сетевому оборудованию, системному программному обеспечению и средствам защиты информации	+	+	+	+	+	+	+	+	+	+
3.2	Обеспечение идентификации и аутентификации пользователей информационной системы	+	+	+	+	+	+	+	+	+	+
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 и контроль за соблюдением правил генерации и смены паролей пользователей информационной системы	+/–	+/–	+/–	+/–	+/–	+/–	+/–	+	+	+
3.7	Обеспечение блокировки доступа к объектам информационной системы после истечения установленного времени бездействия (неактивности) пользователя информационной системы или по его запросу	+	+	+	+	+	+	+	+	+	+
4	Требования по защите системы защиты информации информационной системы										
4.1	Обеспечение изменения атрибутов безопасности сетевого оборудования, системного программного обеспечения и средств защиты информации, установленных по умолчанию	+	+	+	+	+	+	+	+	+	+
4.2	Обеспечение обновления объектов информационной системы	+	+	+	+	+	+	+	+	+	+
4.3	Обеспечение контроля и управления физическим доступом в помещения, в которых постоянно размещаются объекты информационной системы	+	+	+	+	+	+	+	+	+	+
4.4	Обеспечение синхронизации временных меток и (или) системного времени в информационной системе и системе защиты информации	+	+	+	+	+	+	+	+	+	+

5	Обеспечение криптографической защиты информации										
5.1	Обеспечение конфиденциальности и контроля целостности информации при ее передаче посредством сетей электросвязи общего пользования (средства линейного шифрования), если не осуществлено предварительное шифрование защищаемой информации	+/–	+/–	+/–	+/–	+/–	+	+	+	+	+
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 выработки электронной цифровой подписи, средства проверки электронной цифровой подписи, средства выработки личного ключа или открытого ключа электронной цифровой подписи)	+	+	+	+	+	+	+	+	+	+
5.4	Обеспечение контроля целостности данных в информационной системе (средства контроля целостности)	+/–	+/–	+	+/–	+/–	+/–	+/–	+	+/–	+/–
5.5	Обеспечение конфиденциальности и контроля целостности личных ключей, используемых при выработке электронной цифровой подписи (криптографические токены)	+/–	+/–	+/–	+/–	+	+/–	+/–	+/–	+/–	+
5.6	Обеспечение многофакторной и (или) многоэтапной аутентификации пользователей в информационной системе (криптографический токен и (или) средства выработки 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 физической сети, а также виртуальных машин	+/–	+/–	+/–	+/–	+/–	+	+	+	+	+
6.3	Обеспечение безопасного перемещения виртуальных машин и обрабатываемых на них данных	+	+	+	+/–	+/–	+	+	+	+	+
6.4	Обеспечение резервного копирования пользовательских виртуальных машин	+/–	+/–	+	+/–	+	+	+	+	+	+
6.5	Обеспечение резервирования сетевого оборудования по схеме N+1	+/–	+/–	+/–	+/–	+/–	+/–	+/–	+/–	+	+
6.6	Физическая изоляция сегмента виртуальной инфраструктуры (системы хранения и обработки данных), предназначенного для обработки информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам	+/–	+/–	+/–	+/–	+	+/–	+/–	+/–	+/–	+
7	Иные требования										
7.1	Определение перечня разрешенного программного обеспечения и регламентация порядка его установки и использования	+	+	+	+	+	+	+	+	+	+
7.2	Обеспечение контроля за составом объектов информационной системы	+	+	+	+	+	+	+	+	+	+
7.3	Автоматизированный контроль за составом средств вычислительной техники и сетевого оборудования	+/–	+/–	+/–	+/–	+/–	+/–	+/–	+	+	+

7.4	Использование объектов информационной системы под пользовательскими учетными записями (использование административных учетных записей только в случае настройки объектов информационной системы или особенностей объектов информационной системы)	+	+	+	+	+	+	+	+	+	+
7.5	Определение состава и содержания информации, подлежащей резервированию	+	+	+	+	+	+	+	+	+	+
7.6	Обеспечение резервирования информации, подлежащей резервированию	+	+	+	+	+	+	+	+	+	+
7.7	Обеспечение резервирования конфигурационных файлов сетевого оборудования	+/–	+/–	+	+/–	+	+	+	+	+	+
7.8	Обеспечение обновления программного обеспечения объектов информационной системы и контроля за своевременностью такого обновления	+	+	+	+	+	+	+	+	+	+
7.9	Обеспечение сегментирования (изоляции) сети управления объектами информационной системы от сети передачи данных	+/–	+/–	+/–	+/–	+/–	+/–	+/–	+	+	+
7.10	Обеспечение защиты средств вычислительной техники от вредоносных программ	+	+	+	+	+	+	+	+	+	+
7.11	Обеспечение в реальном масштабе времени автоматической проверки пакетов сетевого трафика и файлов данных, передаваемых по сети, и обезвреживание обнаруженных вредоносных программ	+/–	+/–	+/–	+/–	+/–	+/–	+/–	+	+	+
7.12	Обеспечение в реальном масштабе времени автоматической проверки файлов данных, передаваемых по почтовым протоколам, и обезвреживание обнаруженных вредоносных программ	+/–	+/–	+/–	+/–	+/–	+	+	+	+	+
7.13	Обеспечение управления внешними информационными потоками (маршрутизация) между информационными системами. Использование маршрутизатора (коммутатора маршрутизирующего)	+/–	+/–	+/–	+/–	+/–	+	+	+	+	+
7.14	Обеспечение ограничений входящего и исходящего трафика (фильтрация) информационной системы только необходимыми соединениями. Использование межсетевого экрана, функционирующего на канальном, и (или) сетевом, и (или) транспортном, и (или) сеансовом, и (или) прикладном уровнях	+/–	+/–	+/–	+/–	+/–	+	+	+	+	+
7.15	Обеспечение ограничений входящего и исходящего трафика (фильтрация) информационной системы только необходимыми соединениями. Использование межсетевого экрана, функционирующего на канальном, сетевом и прикладном уровнях	+/–	+/–	+/–	+/–	+/–	+	+	+	+	+
7.16	Обеспечение обнаружения и предотвращения вторжений в информационной системе. Использование сетевых, и (или) поведенческих, и (или) узловых систем обнаружения и предотвращения вторжений	+/–	+/–	+/–	+/–	+/–	+	+	+	+	+
7.17	Обеспечение обнаружения и предотвращения вторжений в информационной системе при использовании в ней беспроводных каналов передачи данных (Wi-Fi и тому подобное). Использование беспроводных систем обнаружения и предотвращения вторжений	+/–	+/–	+/–	+/–	+/–	+	+	+	+	+

7.18	Обеспечение обнаружения утечек информации из информационной системы. Использование системы обнаружения утечек информации из информационной системы	+/–	+/–	+/–	+/–	+/–	+/–	+/–	+/–	+/–	+
7.19	Определение перечня внешних подключений к информационной системе и порядка такого подключения	+/–	+/–	+/–	+/–	+/–	+	+	+	+	+
7.20	Обеспечение контроля за внешними подключениями к информационной системе	+/–	+/–	+/–	+/–	+/–	+	+	+	+	+
7.21	Ежегодное проведение внешней и внутренней проверки отсутствия либо невозможности использования нарушителем свойств программных, программно-аппаратных и аппаратных средств, которые могут быть случайно инициированы (активированы) или умышленно использованы для нарушения информационной безопасности системы и сведения о которых подтверждены изготовителями (разработчиками) этих объектов информационной системы	+/–	+/–	+/–	+/–	+/–	+/–	+/–	+	+/–	+

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
12.11.2021 № 195)

ТРЕБОВАНИЯ
к организации взаимодействия информационных систем

	6-частн/6-гос	5-частн/5-гос	4-ин/4-спец/4-бг/4-юл/4-дсп	3-ин/3-спец/3-бг/3-юл/3-дсп
4-ин	х	не допускается	х	не допускается
4-спец	х	не допускается	х	не допускается
4-бг	х	не допускается	х	не допускается
4-юл	х	не допускается	х	не допускается
4-дсп	х	не допускается	х	не допускается
3-ин	не допускается	х/о	не допускается	х/о
3-спец	не допускается	х/о	не допускается	х/о
3-бг	не допускается	х/о	не допускается	х/о
3-юл	не допускается	х/о	не допускается	х/о
3-дсп	не допускается	х/о	не допускается	х/о

Примечания:

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

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

3. Под символом «о» понимается наличие подключения к открытым каналам передачи данных (в том числе к глобальной компьютерной сети Интернет).

Приложение 5
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
12.11.2021 № 195)

МЕТОДЫ
обезличивания персональных данных

1. Для обезличивания персональных данных собственники (владельцы) информационных систем используют следующие методы:

введение идентификаторов;

изменение состава;

декомпозиция;

перестановка;

зашифрование.

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 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 требуется предварительно разработать правила разбиения 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, а также групп записей между собой с последующим раздельным хранением полученных данных и правил изменения.

6. Метод зашифрования реализуется путем применения средств криптографической защиты информации (предварительного шифрования), имеющих сертификат соответствия Национальной системы подтверждения соответствия Республики Беларусь или положительное экспертное заключение по результатам государственной экспертизы, проводимой ОАЦ.

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)