

Государственное бюджетное учреждение
Здравоохранения Пензенской области
«Пензенский областной медицинский
информационно-аналитический центр»
(ГБУЗ МИАЦ)



УТВЕРЖДАЮ
Главный врач ГБУЗ МИАЦ
Н.Н. Ашанина
2014 г.

ПОЛИТИКА информационной безопасности ГБУЗ МИАЦ

Настоящая Политика информационной безопасности государственного бюджетного учреждения здравоохранения Пензенской области «Пензенского областного медицинского информационно-аналитического центра» (далее – Политика), разработана на основе Методических рекомендаций Министерства здравоохранения Российской Федерации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, является официальным документом.

Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности персональных данных изложенных в Концепции информационной безопасности ГБУЗ МИАЦ.

Политика разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и постановления Правительства Российской Федерации от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», на основании:

Приказа Федеральной службы по техническому и экспортному контролю Российской Федерации (далее – ФСТЭК России) от 18.02.2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

Приказа Федеральной службы безопасности Российской Федерации от 10 июля 2014 г. №378 «Об утверждении состава и содержания организационно-технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

«Типовых требований по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных

данных при их обработке в информационных системах персональных данных», утвержденных руководством 8 Центра ФСБ России 21.02.2008 г. № 149/6/6-662;

В Политике определены требования к персоналу информационных систем персональных данных, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в информационных системах персональных данных ГБУЗ МИАЦ.

1.Общие положения

Целью настоящей Политики является обеспечение безопасности информационных систем ГБУЗ МИАЦ от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных и минимизация ущерба от возможной реализации угроз безопасности персональных данных.

Безопасность персональных данных достигается путем исключения несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.

Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на угрозы безопасности персональных данных.

Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

Состав объектов защиты представлен в Перечне персональных данных, подлежащих защите.

Состав информационных систем персональных данных подлежащих защите, представлен в Отчете о результатах проведения внутренней проверки обеспечения режима защиты персональных данных в информационных системах персональных данных ГБУЗ МИАЦ.

2. Область действия

Требования настоящей Политики распространяются на сотрудников ГБУЗ МИАЦ, осуществляющих обработку персональных данных для выполнения своих служебных обязанностей.

3. Система защиты персональных данных

Система защиты персональных данных строится на основании:

- Отчета о результатах проведения внутренней проверки обеспечения режима защиты персональных данных в информационных системах персональных данных ГБУЗ МИАЦ;
- Перечня персональных данных, подлежащих защите в информационных системах персональных данных ГБУЗ МИАЦ;
- Актов определения уровня защищенности информационных систем персональных данных;
- Частных моделей угроз безопасности персональных данных при их обработке в информационных системах персональных данных ГБУЗ МИАЦ;

- Положения о разграничении прав доступа к обрабатываемым персональным данным в ГБУЗ МИАЦ;
- Руководящих документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимый уровень защищенности персональных данных каждой информационной системы персональных данных ГБУЗ МИАЦ. На основании анализа актуальных угроз безопасности персональных данных описанного в Частных моделях угроз безопасности персональных данных при их обработке в информационных системах персональных данных ГБУЗ МИАЦ и Отчете о результатах проведения внутренней проверки обеспечения режима защиты персональных данных в информационных системах персональных данных ГБУЗ МИАЦ, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности персональных данных.

Для каждой информационной системы персональных данных должен быть составлен технический паспорт, содержащий список используемых технических средств защиты, а также информацию о программном обеспечении участвующем в обработке персональных данных, на всех элементах информационной системы персональных данных:

- Автоматизированных рабочих мест пользователей;
- Сервера приложений;
- Систем управления базами данных;
- Границ локально вычислительных сетей;
- Каналов передачи информации в сети общего пользования и международного обмена, если по ним передаются персональные данные.

В зависимости от уровня защищенности информационных систем персональных данных и актуальных угроз, системы защиты персональных данных могут включать следующие средства защиты информации:

- антивирусные средства для рабочих станций пользователей и серверов;
- средства межсетевого экранования;
- средства криптографической защиты информации, при передаче защищаемой информации по каналам связи.

4. Состав и содержание мер по обеспечению безопасности персональных данных

В состав мер по обеспечению безопасности персональных данных, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности персональных данных и применяемых информационных технологий, входят:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;

- защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных);
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности персональных данных;
- обеспечение целостности информационной системы и персональных данных;
- обеспечение доступности персональных данных;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных;
- выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них;
- управление конфигурацией информационной системы и системы защиты персональных данных.

Состав и содержание мер по обеспечению безопасности персональных данных, необходимых для обеспечения каждого из уровней защищенности персональных данных, приведены в Приложении №1 к Политике информационной безопасности ГБУЗ МИАЦ.

4.1 Идентификация и аутентификация субъектов доступа и объектов доступа

Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

4.2 Управление доступом субъектов доступа к объектам доступа

Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль за соблюдением этих правил.

4.3 Ограничение программной среды

Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать

возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

4.4 Защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные (далее - машинные носители персональных данных)

Меры по защите машинных носителей персональных данных (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) должны исключать возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей персональных данных.

4.5 Регистрация событий безопасности

Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также возможность просмотра и анализа информации о таких событиях и реагирование на них.

4.6 Антивирусная защита

Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначеннной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

4.7 Обнаружение (предотвращение) вторжений

Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) персональные данные в целях добывания, уничтожения, искажения и блокирования доступа к персональным данным, а также реагирование на эти действия.

4.8 Контроль (анализ) защищенности персональных данных

Меры по контролю (анализу) защищенности персональных данных должны обеспечивать контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты персональных данных.

4.9 Обеспечение целостности информационной системы и персональных данных

Меры по обеспечению целостности информационной системы и персональных данных должны обеспечивать обнаружение фактов

несанкционированного нарушения целостности информационной системы и содержащихся в ней персональных данных, а также возможность восстановления информационной системы и содержащихся в ней персональных данных.

4.10 Обеспечение доступности персональных данных

Меры по обеспечению доступности персональных данных должны обеспечивать авторизованный доступ пользователей, имеющих права по доступу, к персональным данным, содержащимся в информационной системе, в штатном режиме функционирования информационной системы.

4.11 Защита среды виртуализации

Меры по защите среды виртуализации должны исключать несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

4.12 Защита технических средств

Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.

4.13 Защита информационной системы, ее средств, систем связи и передачи данных

Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных.

4.14 Выявление инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования

информационной системы и (или) к возникновению угроз безопасности персональных данных (далее - инциденты), и реагирование на них

Меры по выявлению инцидентов и реагированию на них должны обеспечивать обнаружение, идентификацию, анализ инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов.

4.15 Управление конфигурацией информационной системы и системы защиты персональных данных

Меры по управлению конфигурацией информационной системы и системы защиты персональных данных должны обеспечивать управление изменениями конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

5. Пользователи информационных систем персональных данных

В Концепции информационной безопасности ГБУЗ МИАЦ определены основные категории пользователей. На основании этих категорий должна быть произведена типизация пользователей информационных систем персональных данных, определен их уровень доступа и возможности.

В информационных системах персональных данных ГБУЗ МИАЦ можно выделить следующие группы пользователей, участвующих в обработке и хранении персональных данных:

- Администратор информационной безопасности;
- Администратор информационной системы персональных данных;
- Пользователь информационной системы персональных данных.

Данные о группах пользователях, уровне их доступа и информированности должен быть отражен в Положении о разграничении прав доступа к обрабатываемым персональным данным.

5.1. Администратор информационной безопасности

Администратор информационной безопасности. Сотрудник ГБУЗ МИАЦ, ответственный за функционирование систем защиты персональных данных, включая настройку и техническое сопровождение систем.

Администратор информационной безопасности обладает следующим уровнем доступа:

- обладает правами Администратора информационной системы персональных данных;
- обладает полной информацией об информационной системе персональных данных;
- имеет доступ к средствам защиты информации и протоколирования и к части ключевых элементов информационной системы персональных данных;
- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

5.2. Пользователь информационной системы персональных данных

Пользователь информационной системы персональных данных, сотрудник ГБУЗ МИАЦ, осуществляющий обработку персональных данных. Обработка персональных данных включает: возможность просмотра персональных данных, ручной ввод персональных данных в информационную систему персональных данных, формирование справок и отчетов по информации, полученной из информационной системы персональных данных. Пользователь не имеет полномочий для управления подсистемами обработки данных и системами защиты персональных данных.

Пользователь информационной системы персональных данных обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми атрибутами и правами, обеспечивающими доступ к персональным данным;
- располагает конфиденциальными данными, к которым имеет доступ.

5.3. Администратор информационной системы персональных данных

Администратор информационной системы персональных данных, сотрудник ГБУЗ МИАЦ, который занимается информационным сопровождением системы.

Администратор информационной системы персональных данных имеет полномочия для управления подсистемами обработки данных но не имеет полномочий для управления средствами защиты персональных данных.

Администратор информационной системы персональных данных обладает следующим уровнем доступа:

- обладает полной информацией о системном и прикладном программном обеспечении информационной системы персональных данных;
- обладает полной информацией о технических средствах и конфигурации информационной системы персональных данных;
- имеет доступ ко всем техническим средствам обработки информации и данным информационной системы персональных данных;
- обладает правами конфигурирования и административной настройки технических средств информационной системы персональных данных.

6. Требования к персоналу по обеспечению защиты персональных данных

Все сотрудники ГБУЗ МИАЦ, являющиеся пользователями информационных систем персональных данных, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности персональных данных.

При вступлении в должность нового сотрудника непосредственный начальник подразделения, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите персональных данных, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования информационных систем персональных данных.

Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами информационных систем персональных данных и систем защиты персональных данных.

Сотрудники ГБУЗ МИАЦ, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать несанкционированного доступа к ним, а также возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Сотрудники ГБУЗ МИАЦ должны следовать установленным процедурам поддержания режима безопасности персональных данных при выборе и использовании паролей (если не используются технические средства аутентификации).

Сотрудники ГБУЗ МИАЦ должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица. Все пользователи должны знать требования по безопасности персональных данных и процедуры защиты оборудования, оставленного без присмотра, а также свои обязанности по обеспечению такой защиты.

Сотрудникам запрещается устанавливать постороннее программное обеспечение, подключать личные мобильные устройства и носители информации, а также записывать на них защищаемую информацию.

Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами ГБУЗ МИАЦ, третьим лицам.

При работе с персональными данными в информационных системах персональных данных сотрудники ГБУЗ МИАЦ обязаны обеспечить отсутствие возможности просмотра персональных данных третьими лицами с мониторов автоматизированных рабочих мест или терминалов.

При завершении работы с информационными системами персональных данных сотрудники обязаны защитить автоматизированные рабочие места или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты.

Сотрудники ГБУЗ МИАЦ должны быть проинформированы об угрозах нарушения режима безопасности персональных данных и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятую политику и процедуры безопасности персональных данных.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы информационных систем персональных данных, которые могут повлечь за собой угрозы безопасности персональных данных, а также о выявленных ими событиях, затрагивающих безопасность персональных данных, руководству подразделения и лицу, отвечающему за немедленное реагирование на угрозы безопасности персональных данных.

7. Должностные обязанности пользователей информационной системы персональных данных

Должностные обязанности пользователей информационной системы персональных данных описаны в следующих документах:

- Инструкция администратора информационной безопасности;
- Инструкция администратора информационной системы персональных данных;
- Инструкция пользователя информационной системы персональных данных;
- Инструкция пользователя информационной системы персональных данных по обеспечению безопасности обработки персональных данных при возникновении внештатных ситуаций.

8. Ответственность сотрудников информационной системы персональных данных ГБУЗ МИАЦ

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут граждансскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

Действующее законодательство Российской Федерации позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации электронно-вычислительных машин и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы электронно-вычислительных машин или сетей (статьи 272,273 и 274 УК РФ).

Администратор информационной системы персональных данных и Администратор информационной безопасности несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

При нарушениях сотрудниками ГБУЗ МИАЦ – пользователями информационных систем персональных данных правил, связанных с безопасностью персональных данных, они несут ответственность, установленную действующим законодательством Российской Федерации.

Необходимо внести в Положения о подразделениях ГБУЗ МИАЦ, осуществляющих обработку персональных данных в информационных системах персональных данных сведения об ответственности их руководителей и сотрудников за разглашение и несанкционированную модификацию (искажение, фальсификацию) персональных данных, а также за неправомерное вмешательство в процессы их автоматизированной обработки.

9. Список использованных источников

Основными нормативно-правовыми и методическими документами, на которых базируется настоящая Политика являются:

1. Федеральный Закон от 27.07.2006 г. № 152-ФЗ «О персональных данных» (далее – ФЗ «О персональных данных»), устанавливающий основные принципы и условия обработки персональных данных, права, обязанности и ответственность участников отношений, связанных с обработкой персональных данных.

2. Постановление Правительства Российской Федерации от 01.11.2012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

3. «Положение об особенностях обработки персональных данных, осуществляющейся без использования средств автоматизации», утвержденное Постановлением Правительства РФ от 15.09.2008 г. № 687.

4. «Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных», утвержденные Постановлением Правительства РФ от 06.07.2008 г. №512 (В ред. Постановления Правительства РФ от 27.12.2012 №1404).

5. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г.

6. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Зам. директора ФСТЭК России 15.02.08 г.

7. «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденные руководством 8 Центра ФСБ России 21.02.2008 г. № 149/6/6-662.

8. Приказ ФСТЭК России от 18.02.2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

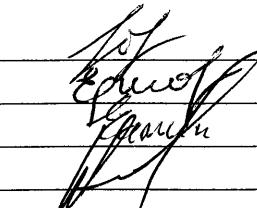
9. Приказ ФСБ России от 10.07.2014 г. №378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

Ведущий инженер по защите информации

Ведущий инженер по защите информации

Инженер-программист

Заместитель главного врача


Юров А.Н.
Ершов С.В.
Чамин И.О.
Жиляев П.С.

Приложение №1 к Политике
информационной безопасности

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищенности персональных данных			
		4	3	2	1
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)					
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	+	+	+
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных			+	+
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+	+	+	+
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+	+	+	+
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+	+	+	+
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+	+	+	+
II. Управление доступом субъектов доступа к объектам доступа (УПД)					
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей	+	+	+	+
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+	+	+	+
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, односторонняя передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	+	+	+	+
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	+	+	+	+
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	+	+	+	+
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	+	+	+	+
УПД.7	Предупреждение пользователя при его входе в информационную систему о том, что в информационной системе реализованы меры по обеспечению безопасности персональных данных, и о необходимости соблюдения установленных оператором правил обработки персональных данных				
УПД.8	Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему				
УПД.9	Ограничение числа параллельных сессий доступа для каждой учетной записи пользователя информационной системы				
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу		+	+	+

УПД.11	Разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации		+	+	+
УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе ее хранения и обработки				
УПД.13	Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	+	+	+	+
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	+	+	+	+
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	+	+	+	+
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	+	+	+	+
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники			+	+
III. Ограничение программной среды (ОПС)					
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения				
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения			+	+
ОПС.3	Установка (инсталляция) только разрешенного к использованию программного обеспечения и (или) его компонентов				+
ОПС.4	Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов				
IV. Защита машинных носителей персональных данных (ЗНИ)					
ЗНИ.1	Учет машинных носителей персональных данных			+	+
ЗНИ.2	Управление доступом к машинным носителям персональных данных			+	+
ЗНИ.3	Контроль перемещения машинных носителей персональных данных за пределы контролируемой зоны				
ЗНИ.4	Исключение возможности несанкционированного ознакомления с содержанием персональных данных, хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных системах				
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных				
ЗНИ.6	Контроль ввода (вывода) информации на машинные носители персональных данных				
ЗНИ.7	Контроль подключения машинных носителей персональных данных				
ЗНИ.8	Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания		+	+	+
V. Регистрация событий безопасности (РСБ)					

РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+	+	+	+
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+	+	+	+
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+	+	+	+
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти				
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них			+	+
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе				
РСБ.7	Защита информации о событиях безопасности	+	+	+	+
VI. Антивирусная защита (АВЗ)					
АВЗ.1	Реализация антивирусной защиты	+	+	+	+
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+	+	+
VII. Обнаружение вторжений (СОВ)					
СОВ.1	Обнаружение вторжений			+	+
СОВ.2	Обновление базы решающих правил			+	+
VIII. Контроль (анализ) защищенности персональных данных (АНЗ)					
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей		+	+	+
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+	+	+	+
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации		+	+	+
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации		+	+	+
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе			+	+
IX. Обеспечение целостности информационной системы и персональных данных (ОЦЛ)					
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации			+	+
ОЦЛ.2	Контроль целостности персональных данных, содержащихся в базах данных информационной системы			*	
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций				
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)			+	+

ОЦЛ.5	Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещенной к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы				
ОЦЛ.6	Ограничение прав пользователей по вводу информации в информационную систему				
ОЦЛ.7	Контроль точности, полноты и правильности данных, вводимых в информационную систему				
ОЦЛ.8	Контроль ошибочных действий пользователей по вводу и (или) передаче персональных данных и предупреждение пользователей об ошибочных действиях				
Х. Обеспечение доступности персональных данных (ОДТ)					
ОДТ.1	Использование отказоустойчивых технических средств				
ОДТ.2	Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы				
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование				+
ОДТ.4	Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных			+	+
ОДТ.5	Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала			+	+
XI. Защита среды виртуализации (ЗСВ)					
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	+	+	+	+
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	+	+	+	+
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре	+	+	+	+
ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, односторонняя передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры				
ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией				
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных			+	+
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций			+	+
ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры			+	+
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре		+	+	+

ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей		+	+	+
XII. Защита технических средств (ЗТС)					
ЗТС.1	Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам				
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования				
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены	+	+	+	+
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр	+	+	+	+
ЗТС.5	Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)				
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)					
ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций информационной системы				+
ЗИС.2	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом				
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи	+	+	+	+
ЗИС.4	Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)				
ЗИС.5	Запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств				
ЗИС.6	Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с персональными данными, при обмене ими с иными информационными системами				
ЗИС.7	Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода				

ЗИС.8	Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи			
ЗИС.9	Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации			
ЗИС.10	Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имен по сетевым адресам			
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов		+	+
ЗИС.12	Исключение возможности отрицания пользователем факта отправки персональных данных другому пользователю			
ЗИС.13	Исключение возможности отрицания пользователем факта получения персональных данных от другого пользователя			
ЗИС.14	Использование устройств терминального доступа для обработки персональных данных			
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных		+	+
ЗИС.16	Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер или внутри разрешенных сетевых протоколов			
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы		+	+
ЗИС.18	Обеспечение загрузки и исполнения программного обеспечения с машинных носителей персональных данных, доступных только для чтения, и контроль целостности данного программного обеспечения			
ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти			
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе	+	+	+
XIV. Выявление инцидентов и реагирование на них (ИНЦ)				
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них		+	+
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов		+	+
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами		+	+
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий		+	+

ИНЦ.5	Принятие мер по устранению последствий инцидентов			+	+
ИНЦ.6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов			+	+
XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)					
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных		+	+	+
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных		+	+	+
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных		+	+	+
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных		+	+	+

«+» - мера по обеспечению безопасности персональных данных включена в базовый набор мер для соответствующего уровня защищенности персональных данных.

Меры по обеспечению безопасности персональных данных, не обозначенные знаком «+», применяются при адаптации базового набора мер и уточнении адаптированного базового набора мер, а также при разработке компенсирующих мер по обеспечению безопасности персональных данных.