

УТВЕРЖДАЮ

00.00.0000г

Руководитель ООО «ААА»

\_\_\_\_\_  
Фамилия И.О.1

Базовая модель угроз безопасности  
персональных данных при их обработке  
в информационных системах ООО «ААА»

1. Общие положения

1.1. Настоящая Базовая модель угроз безопасности персональных данных при их обработке в информационных системах (далее - Базовая модель) Общества с ограниченной ответственностью «ААА» (далее - организация) разработана на основе Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", Федерального закона от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации", Постановления Правительства Российской Федерации от 01.11.2012 N 1119 "Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных", "ГОСТ Р 59407-2021. Национальный стандарт Российской Федерации. Информационные технологии. Методы и средства обеспечения безопасности. Базовая архитектура защиты персональных данных" (утв. и введен в действие Приказом Росстандарта от 20.05.2021 N 415-ст), "ГОСТ ISO/IEC 29100-2021. Межгосударственный стандарт. Информационные технологии. Методы и средства обеспечения безопасности. Основы защиты персональных данных" (введен в действие Приказом Росстандарта от 02.07.2021 N 610-ст), ГОСТ Р 51275-2006. Национальный стандарт Российской Федерации. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения (утвержден и введен в действие Приказом Ростехрегулирования от 27.12.2006 N 374-ст), ГОСТ Р 56205-2014/IEC/TS 62443-1-1:2009. Национальный стандарт Российской Федерации. Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели (утвержден и введен в действие Приказом Росстандарта от 10.11.2014 N 1493-ст), ГОСТ Р ИСО/МЭК 27033-1-2011. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции (утвержден и введен в действие Приказом Росстандарта от 01.12.2011 N 683-ст), ГОСТ Р 50739-95. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования (принят и введен в действие Постановлением Госстандарта России от 09.02.1995 N 49), ГОСТ Р 50922-2006. Защита информации. Основные термины и определения (утвержден и введен в действие Приказом Ростехрегулирования от 27.12.2006 N 373-ст), ГОСТ Р 56545-2015. Национальный стандарт Российской Федерации. Защита информации. Уязвимости информационных систем. Правила описания уязвимостей (утвержден и введен в действие Приказом Росстандарта от 19.08.2015 N 1180-ст), ГОСТ Р 56546-2015. Национальный стандарт Российской Федерации. Защита информации. Уязвимости информационных систем. Классификация уязвимостей информационных систем (утвержден и введен в действие Приказом Росстандарта от 19.08.2015 N 1181-ст), ГОСТ Р 56938-2016. Национальный стандарт Российской Федерации. Защита информации. Защита информации при использовании технологий виртуализации. Общие положения (утвержден и введен в действие Приказом Росстандарта от 01.06.2016 N 457-ст), ГОСТ Р ИСО/МЭК ТО 18044-2007.

Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности (утвержден Приказом Ростехрегулирования от 27.12.2007 N 513-ст), ГОСТ Р ИСО/МЭК 15408-3-2013. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности (утвержден Приказом Ростехрегулирования от 27.12.2007 N 513-ст).

1.2. Базовая модель содержит систематизированный перечень угроз и мер по обеспечению безопасности персональных данных при их обработке в информационных системах организации. Эти угрозы обусловлены преднамеренными или непреднамеренными действиями физических лиц, действиями зарубежных спецслужб или организаций (в том числе террористических), а также криминальных группировок, создающих условия (предпосылки) для нарушения безопасности персональных данных, которое ведет к ущербу жизненно важных интересов организации, личностей, общества. Угрозы рассматриваются в качестве рисков снижения безопасности персональных данных.

1.3. Для целей настоящей Базовой модели персональные данные рассматриваются как один из видов информации, относящейся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

## 2. Обозначения и сокращения

В Базовой модели применены следующие сокращения:

- АРМ - автоматизированное рабочее место;
- АС - автоматизированная система;
- ПДн - персональные данные;
- ИСПДн - информационные системы персональных данных;
- МИС – медицинская информационная система;
- МНИ - машинные носители информации;
- НСД - несанкционированный доступ;
- ПО - программное обеспечение;
- СКЗИ - средства криптографической защиты информации;
- СВТ - средство вычислительной техники;
- СУБД - система управления базами данных.

## 3. Термины и определения

В Базовой модели применены термины в соответствии с Федеральным законом от 27.07.2006 N 149-ФЗ "Об информации, информационных технологиях и о защите информации", Федеральным законом от 27.07.2006 N 152-ФЗ "О персональных данных", "ГОСТ Р 59407-2021. Национальный стандарт Российской Федерации. Информационные технологии. Методы и средства обеспечения безопасности. Базовая архитектура защиты персональных данных" (утв. и введен в действие Приказом Росстандарта от 20.05.2021 N 415-ст), "ГОСТ ISO/IEC 29100-2021. Межгосударственный

стандарт. Информационные технологии. Методы и средства обеспечения безопасности. Основы защиты персональных данных" (введен в действие Приказом Росстандарта от 02.07.2021 N 610-ст), ГОСТ Р 51275-2006. Национальный стандарт Российской Федерации. Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения, а также следующие термины с соответствующими определениями:

3.1. Атрибуты, используемые для идентификации физического лица, обрабатываемые в информационных системах:

возраст;

любая информация, собранная во время оказания медицинских услуг;

номер банковского счета или кредитной карты;

биометрический идентификатор;

информация о дебетовой или кредитной банковской карте;

**сведения из кредитной истории;**

дата рождения;

информация о диагностике состояния здоровья;

нетрудоспособность;

документ о нетрудоспособности;

финансовая информация, связанная с взаиморасчетами при оказании платных медицинских услуг;

пол;

данные GPS о местоположении устройства при посещении сайта;

траектории GPS устройства при посещении сайта;

домашний адрес и иные адреса, предоставляемые лицом при оказании платных медицинских услуг;

IP-адрес;

информация о местоположении, полученная от телекоммуникационных систем;

данные медицинской карты;

фамилия, имя, отчество;

государственные идентификаторы, например номер и серия паспорта;

адрес личной электронной почты;

личные идентификационные номера (PIN-коды) или пароли;

личные интересы, полученные из отслеживания web-сайтов Интернета;

личный или поведенческий стереотип;

номер личного телефона;

фотография или видео, по которым можно идентифицировать человека;

предпочтения, касающиеся продуктов и услуг;

расовое или этническое происхождение;

3.2. Объект информатизации: совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

3.3. Система обработки информации: совокупность технических средств и программного обеспечения, а также методов обработки информации и действий персонала, необходимых для выполнения автоматизированной обработки информации.

3.4. Вредоносная программа: программа, используемая для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы автоматизированной информационной системы.

3.5. Актуальные угрозы безопасности персональных данных - это совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.

Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.

Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.

Определение типа угроз безопасности персональных данных, актуальных для информационной системы, производится с учетом оценки возможного вреда, проведенной во исполнение п. 5 ч. 1 ст. 18.1 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных", и в соответствии с нормативными правовыми актами, принятыми во исполнение ч. 5 ст. 19 Федерального закона от 27.07.2006 N 152-ФЗ "О персональных данных".

3.6. (Компьютерный) вирус: вредоносная программа, способная создавать свои копии и (или) другие вредоносные программы.

3.7. Компьютерная атака: целенаправленное несанкционированное воздействие на информацию, на ресурс автоматизированной информационной системы или получение несанкционированного доступа к ним с применением программных или программно-аппаратных

средств.

3.8. Сетевая атака: компьютерная атака с использованием протоколов межсетевого взаимодействия.

3.9. Программное воздействие: несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

3.10. Меры защиты информации: организационные (в том числе управленческие) и технические меры, применяемые для защиты информации и обеспечения доступности АС.

3.11. Техническая мера защиты информации: мера защиты информации, реализуемая с помощью применения аппаратных, программных, аппаратно-программных средств и (или) систем.

3.12. Организационная мера защиты информации: мера, не являющаяся технической мерой защиты информации, предусматривающая установление временных, территориальных, пространственных, правовых, методических и иных ограничений на условия использования и режимы работы объекта информатизации и (или) иных связанных с ним объектов.

3.13. Система защиты информации: совокупность мер защиты информации, применение которых направлено на непосредственное обеспечение защиты информации, процессов применения указанных мер защиты информации, ресурсного и организационного обеспечения, необходимого для применения указанных мер защиты информации.

3.14. Система организации и управления защитой информации: совокупность мер защиты информации, применение которых направлено на обеспечение полноты и качества защиты информации, предназначенных для планирования, реализации, контроля и совершенствования процессов системы защиты информации.

3.15. Объект доступа: объект информатизации, представляющий собой аппаратное средство, средство вычислительной техники и (или) сетевое оборудование, в том числе входящие в состав АС организации.

Примечание. В составе основных типов объектов доступа рассматриваются:

- автоматизированные рабочие места (АРМ) пользователей;
- АРМ эксплуатационного персонала;
- серверное оборудование;
- сетевое оборудование;
- системы хранения данных;
- аппаратные модули безопасности (HSM);
- устройства печати и копирования информации.

3.16. Ресурс доступа: объект информатизации, представляющий собой совокупность информации и программного обеспечения (ПО) обработки информации.

Примечание. В составе основных типов ресурсов доступа рекомендуется как минимум рассматривать:

- АС;
- базы данных;
- сетевые файловые ресурсы;
- виртуальные машины, предназначенные для размещения серверных компонентов АС;
- виртуальные машины, предназначенные для размещения АРМ пользователей и эксплуатационного персонала;
- ресурсы доступа, относящиеся к сервисам электронной почты;
- ресурсы доступа, относящиеся к WEB-сервисам организации в сетях Интранет и Интернет.

3.17. Контур безопасности: совокупность объектов информатизации, определяемая областью применения Базовой модели, используемых для реализации бизнес-процессов и (или) технологических процессов организации единой степени критичности (важности), для которой организацией применяется единая политика (режим) защиты информации (единый набор требований к обеспечению защиты информации).

3.18. Уровень защиты информации: определенная совокупность мер защиты информации, входящих в состав системы защиты информации и системы организации и управления защитой информации, применяемых совместно в пределах контура безопасности для реализации политики (режима) защиты информации, соответствующей критичности (важности) защищаемой информации бизнес-процессов и (или) технологических процессов организации.

3.19. Физический доступ к объекту доступа (физический доступ): доступ к объекту доступа, включая доступ в помещение, в котором расположен объект доступа, позволяющий осуществить физическое воздействие на него.

3.20. Логический доступ к ресурсу доступа (логический доступ): доступ к ресурсу доступа, в том числе удаленный, реализуемый с использованием вычислительных сетей, позволяющий, в том числе без физического доступа, осуществить доступ к защищаемой информации или выполнить операции по обработке защищаемой информации.

3.21. Субъект доступа: работник организации или иное лицо, осуществляющий физический и (или) логический доступ, или программный сервис, осуществляющий логический доступ.

Примечание. В составе основных типов субъектов доступа рассматриваются:

- пользователи - субъекты доступа, в том числе клиенты организации, осуществляющие доступ к объектам и (или) ресурсам доступа с целью использования услуг, предоставляемых информационной инфраструктурой организации;

- эксплуатационный персонал - субъекты доступа, в том числе представители подрядных организаций, которые решают задачи обеспечения эксплуатации и (или) администрирования объектов и (или) ресурсов доступа, для которых необходимо осуществление логического доступа, включая задачи, связанные с эксплуатацией и администрированием технических мер защиты информации;

- технический (вспомогательный) персонал - субъекты доступа, в том числе представители подрядных организаций, решающие задачи, связанные с обеспечением эксплуатации объектов доступа, для выполнения которых не требуется осуществление логического доступа, или

выполняющие хозяйственную деятельность и осуществляющие физический доступ к объектам доступа без цели их непосредственного использования;

- программные сервисы - процессы выполнения программ в информационной инфраструктуре, осуществляющие логический доступ к ресурсам доступа.

3.22. Авторизация: проверка, подтверждение и предоставление прав логического доступа при осуществлении субъектами доступа логического доступа.

3.23. Идентификация: присвоение для осуществления логического доступа субъекту (объекту) доступа уникального признака (идентификатора); сравнение при осуществлении логического доступа предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов.

3.24. Аутентификация: проверка при осуществлении логического доступа принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

3.25. Регистрация событий защиты информации (регистрация): фиксация данных о совершенных субъектами доступа действиях или данных о событиях защиты информации.

3.26. Учетная запись: логический объект (информация), существующий в пределах одного или нескольких ресурсов доступа и представляющий субъекта доступа в его (их) пределах.

3.27. Техническая учетная запись: учетная запись, используемая для осуществления логического доступа программными сервисами.

3.28. Права логического доступа: набор действий, разрешенных для выполнения субъектом доступа над ресурсом доступа с использованием соответствующей учетной записи.

3.29. Роль логического доступа (роль): заранее определенная совокупность функций и задач субъекта доступа, для выполнения которых необходим определенный набор прав логического доступа.

3.30. Роль защиты информации: заранее определенная совокупность функций и задач субъекта доступа, в том числе работника организации, связанных с применением организационных и (или) технических мер защиты информации.

3.31. Легальный субъект доступа: субъект доступа, наделенный организацией полномочиями на осуществление физического и (или) логического доступа.

3.32. Аутентификационные данные: данные в любой форме и на любом носителе, известные или принадлежащие легальному субъекту доступа - легальному владельцу аутентификационных данных, или данные, которыми обладает легальный субъект доступа, используемые для выполнения процедуры аутентификации при осуществлении логического доступа.

3.33. Компрометация аутентификационных данных: событие, связанное с возникновением возможности использования аутентификационных данных субъектом, не являющимся легальным владельцем указанных аутентификационных данных.

3.34. Фактор аутентификации: блок данных, используемых при аутентификации субъекта или объекта доступа.

Примечание. Факторы аутентификации подразделяются на следующие три категории:

- что-то, что субъект или объект доступа знает, например пароли легальных субъектов доступа, ПИН-коды;

- что-то, чем субъект или объект доступа обладает, например данные, хранимые на персональных технических устройствах аутентификации: токенах, смарт-картах и иных носителях;

- что-то, что свойственно субъекту или объекту доступа, например биометрические данные физического лица - легального субъекта доступа.

3.35. Событие защиты информации: идентифицированное возникновение и (или) изменение состояния объектов информатизации организации, действия работников организации и (или) иных лиц, указывающие на возможный (потенциальный) инцидент, связанный с реализацией информационных угроз.

3.36. Инцидент защиты информации: одно или серия связанных нежелательных или неожиданных событий защиты информации, которые могут привести к риску нарушения выполнения бизнес-процессов, технологических процессов организации и (или) нарушить безопасность информации.

Примечание. В составе типов инцидентов защиты информации рассматриваются:

- несанкционированный доступ к информации;
- нарушение в обеспечении защиты информации, включая нарушение работы технических мер защиты информации, появление уязвимостей защиты информации;
- нарушение требований законодательства Российской Федерации, в том числе нормативных актов, внутренних документов организации в области обеспечения защиты информации;
- нарушение регламентированных сроков выполнения процедур и операций в рамках предоставления услуг;
- нарушение установленных показателей предоставления услуг;
- нанесение финансового ущерба организации, ее клиентам и контрагентам;
- выполнение операций (транзакций), приводящих к финансовым последствиям организации, ее клиентов и контрагентов, осуществление переводов денежных средств по распоряжению лиц, не обладающих соответствующими полномочиями, или с использованием искаженной информации, содержащейся в соответствующих распоряжениях (электронных сообщениях).

3.37. Управление инцидентами защиты информации: деятельность по своевременному обнаружению инцидентов защиты информации, адекватному и оперативному реагированию на них, направленная на минимизацию и (или) ликвидацию негативных последствий от инцидентов защиты информации для организации и (или) ее клиентов, а также на снижение вероятности повторного возникновения инцидентов защиты информации.

3.38. Группа реагирования на инциденты защиты информации; ГРИЗИ: действующая на постоянной основе группа работников организации и (или) иных лиц, привлекаемых ею, которая выполняет регламентированные в организации процедуры реагирования на инциденты защиты информации.

3.39. Информация конфиденциального характера: информация, для которой в соответствии с законодательством Российской Федерации, в том числе нормативными актами, и (или)

внутренними документами организации обеспечивается сохранение свойства конфиденциальности.

3.40. Утечка информации: неконтролируемое организацией распространение информации конфиденциального характера.

3.41. Защита информации от утечки: защита информации, направленная на предотвращение неконтролируемого организацией распространения информации конфиденциального характера.

3.42. Ресурс персональных данных: база данных или иная совокупность персональных данных (ПДн) многих субъектов ПДн, объединенных общими целями обработки, обрабатываемых организацией с использованием или без использования объектов информатизации, в том числе АС.

3.43. Управление рисками - скоординированные действия по руководству и управлению информационной безопасностью в отношении ПДн.

#### 4. Общие положения

4.1. Соблюдение принципа обеспечения информационной безопасности означает:

- защиту ПДн в рамках своих полномочий с помощью соответствующих мер обеспечения безопасности на эксплуатационном, функциональном и стратегическом уровне для обеспечения их целостности, конфиденциальности и доступности, а также защиту от рисков, таких как несанкционированный доступ, разрушение, использование, модификация или раскрытие либо потеря в течение всего их жизненного цикла;

- выбор обработчиков ПДн, которые предоставляют достаточные гарантии как относительно организационных, физических и технических мер обеспечения безопасности обработки ПДн, так и относительно обеспечения соответствия этим мерам;

- базирование мер обеспечения безопасности ПДн на требованиях соответствующего законодательства, стандартов безопасности, а также результатах систематических оценок рисков безопасности, как описано в ГОСТ Р ИСО 31000-2019 "Национальный стандарт Российской Федерации. Менеджмент риска. Принципы и руководство" (утв. и введен в действие Приказом Росстандарта от 10.12.2019 N 1379-ст), и результатах анализа "затраты/выгода";

- реализацию мер обеспечения безопасности соразмерно вероятности и серьезности потенциальных последствий, чувствительности ПДн, числу субъектов ПДн, которые могут быть затронуты, и контексту, в котором она производится;

- ограничение доступа к ПДн для пользователей, кроме тех лиц, кому такой доступ требуется для выполнения своих обязанностей, и ограничение доступа лицам, имеющим доступ к ПДн, только к той части ПДн, которые им необходимы для выполнения своих обязанностей;

- принятие решений относительно рисков и уязвимостей, обнаруженных с помощью оценок риска обеспечения защиты ПДн и процессов аудита;

- периодический пересмотр и переоценка мер обеспечения безопасности ПДн в процессе постоянного управления рисками безопасности.

4.2. Принципы обеспечения безопасности ПДн:

согласие и выбор;

законность цели и ее спецификация;

ограничение на сбор информации;

минимизация данных;

ограничения в отношении использования, хранения и раскрытия;

точность и качество;

открытость, прозрачность и уведомление;

индивидуальное участие и доступ;

ответственность;

информационная безопасность;

соответствие безопасности ПДн.

4.3. Процесс управления рисками защиты ПДн включает в себя следующие процессы:

- установление контекста путем осмысления организации (например, обработка ПДн, обязанности), технической среды и факторов, влияющих на управление рисками нарушения безопасности ПДн (т.е. правовые и нормативные факторы, договорные факторы, факторы бизнеса и другие факторы);

- оценку риска путем идентификации, анализа и оценивания рисков для субъектов ПДн (риски, которые могут повлиять на них неблагоприятным образом);

- обработку риска путем определения требований по защите ПДн, идентификации и реализации мер обеспечения безопасности ПДн для предотвращения или уменьшения рисков для субъектов ПДн;

- коммуникации и консультирование путем получения информации от заинтересованных сторон, достижения согласия по каждому процессу управления рисками, а также информирования субъектов ПДн и сообщения им о рисках и мерах обеспечения безопасности ПДн;

- мониторинг и пересмотр путем отслеживания рисков, мер обеспечения безопасности ПДн, а также усовершенствования процесса.

Одним из результатов может быть оценка влияния защиты ПДн, которая является составной частью управления рисками, направленного на обеспечение соблюдения законодательных требований в части защиты ПДн, и оценка последствий обеспечения защиты ПДн в новых или существенно измененных программах или видах деятельности. Оценки влияния защиты ПДн должны быть оформлены в рамках более широкой структуры управления рисками организации.

4.4. 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.

4.4.1. 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).

4.4.2. 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.

4.4.3. 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.

4.4.4. 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.

4.4.5. 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.

4.4.6. Меры по антивирусной защите должны обеспечивать обнаружение в информационной

системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

4.4.7. 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.

4.4.8. 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.

4.4.9. 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.

4.4.10. 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.

4.4.11. 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.

4.4.12. 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.

4.4.13. 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.

4.4.14. 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.

4.4.15. 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.

4.5. Выбор мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе в рамках системы защиты персональных данных, включает:

определение базового набора мер по обеспечению безопасности персональных данных для установленного уровня защищенности персональных данных в соответствии с базовыми наборами мер по обеспечению безопасности персональных данных, приведенными в Приложении N \_\_\_\_ к настоящему документу;

адаптацию базового набора мер по обеспечению безопасности персональных данных с учетом структурно-функциональных характеристик информационной системы, информационных технологий, особенностей функционирования информационной системы (в том числе исключение из базового набора мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе);

уточнение адаптированного базового набора мер по обеспечению безопасности персональных данных с учетом не выбранных ранее мер, приведенных в Приложении N \_\_\_\_ к настоящему документу, в результате чего определяются меры по обеспечению безопасности персональных данных, направленные на нейтрализацию всех актуальных угроз безопасности персональных данных для конкретной информационной системы;

дополнение уточненного адаптированного базового набора мер по обеспечению безопасности персональных данных мерами, обеспечивающими выполнение требований к защите персональных данных, установленными иными нормативными правовыми актами в области обеспечения безопасности персональных данных и защиты информации.

4.6. При невозможности технической реализации отдельных выбранных мер по обеспечению безопасности персональных данных, а также с учетом экономической целесообразности на этапах адаптации базового набора мер и (или) уточнения адаптированного базового набора мер могут разрабатываться иные (компенсирующие) меры, направленные на нейтрализацию актуальных угроз безопасности персональных данных.

В этом случае в ходе разработки системы защиты персональных данных должно быть проведено обоснование применения компенсирующих мер для обеспечения безопасности персональных данных.

4.7. Технические меры защиты персональных данных реализуются посредством применения средств защиты информации, в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности.

При использовании в информационных системах сертифицированных по требованиям безопасности информации средств защиты информации:

в информационных системах 1 уровня защищенности персональных данных применяются средства защиты информации не ниже 4 класса и 4 уровня доверия, а также средства вычислительной техники не ниже 5 класса;

в информационных системах 2 уровня защищенности персональных данных применяются средства защиты информации не ниже 5 класса и 5 уровня доверия, а также средства вычислительной техники не ниже 5 класса;

в информационных системах 3 уровня защищенности персональных данных применяются средства защиты информации 6 класса и 6 уровня доверия, а также средства вычислительной техники не ниже 5 класса;

в информационных системах 4 уровня защищенности персональных данных применяются средства защиты информации 6 класса и 6 уровня доверия, а также средства вычислительной техники не ниже 6 класса.

Классы защиты определяются в соответствии с нормативными правовыми актами, изданными в соответствии с пп. 13.1 п. 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16.09.2004 N 1085.

Уровни доверия устанавливаются в соответствии с Требованиями по безопасности информации, устанавливающими уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий (выписка), утвержденными Приказом ФСТЭК России от 02.06.2020 N 76.

При использовании в информационных системах средств защиты информации, сертифицированных по требованиям безопасности информации, указанные средства должны быть сертифицированы на соответствие обязательным требованиям по безопасности информации, установленным нормативными правовыми актами, или требованиям, указанным в технических условиях (заданиях по безопасности).

Функции безопасности средств защиты информации должны обеспечивать выполнение мер по обеспечению безопасности персональных данных, содержащихся в настоящей Базовой модели.

## 5. Виды угроз и меры их нейтрализации

5.1. Базовая модель разработана с учетом того, что из всех возможных объектов атак персональных данных нарушитель с наибольшей вероятностью выберет наиболее слабо контролируемый, где его деятельность будет оставаться необнаруженной максимально долго. Поэтому все критические операции, где осуществляется любое взаимодействие субъектов доступа с объектами информатизации, должны особенно тщательно контролироваться.

5.2. Основными типами источников угроз безопасности персональных данных являются:

- неблагоприятные события техногенного характера;
- сбои и отказы в работе объектов и (или) ресурсов доступа;
- зависимость процессов эксплуатации объектов информатизации от иностранных поставщиков или провайдеров услуг;
- внутренние нарушители безопасности информации - лица, в том числе работники организации и работники подрядных организаций, реализующие угрозы безопасности информации с использованием легально предоставленных им прав логического или физического доступа;
- внешние нарушители безопасности информации - лица, в том числе работники организации, реализующие угрозы безопасности информации без использования легально предоставленных прав

логического или физического доступа, а также субъекты, не являющиеся работниками организации, реализующие целенаправленные компьютерные атаки, в том числе с целью личного обогащения или блокирования штатного функционирования бизнес-процессов или технологических процессов организации.

5.3. К числу наиболее актуальных источников угроз на уровне аппаратного обеспечения, уровне сетевого оборудования и уровне сетевых приложений и сервисов относятся следующие:

- сбои и отказы в работе объектов доступа;
- внутренние нарушители безопасности информации (эксплуатационный, вспомогательный (технический) персонал), осуществляющие целенаправленное деструктивное воздействие на объекты доступа;
- зависимость процессов эксплуатации объектов доступа от иностранных поставщиков или провайдеров услуг;
- внешние нарушители безопасности информации, обладающие знаниями о возможных уязвимостях защиты информации;
- внешние нарушители безопасности информации, организующие DoS, DDoS и иные виды компьютерных атак;
- комбинированные источники угроз: внешние и внутренние нарушители безопасности информации, действующие совместно и (или) согласованно.

5.4. К числу наиболее актуальных источников угроз на уровне серверных компонентов виртуализации, программных инфраструктурных сервисов, операционных систем, систем управления базами данных и серверов приложений относятся следующие:

- внутренние нарушители безопасности информации (эксплуатационный персонал), осуществляющие целенаправленные деструктивные воздействия на ресурсы доступа;
- внутренние нарушители безопасности информации (эксплуатационный персонал), реализующие угрозы безопасности информации с использованием легально предоставленных прав логического доступа;
- сбои и отказы в работе ПО;
- зависимость процессов эксплуатации ресурсов доступа, ПО от иностранных поставщиков или провайдеров услуг;
- внешние нарушители безопасности информации, обладающие знаниями о возможных уязвимостях защиты информации;
- комбинированные источники угроз: внешние и внутренние нарушители безопасности информации, действующие в сговоре.

5.5. К числу наиболее актуальных источников угроз на уровне АС и приложений, эксплуатируемых в рамках бизнес-процессов и технологических процессов организации, относятся следующие:

- внутренние нарушители безопасности информации (пользователи и эксплуатационный персонал АС и приложений), реализующие угрозы безопасности информации с использованием

легально предоставленных прав логического доступа;

- внешние нарушители безопасности информации, обладающие знаниями о возможных уязвимостях защиты информации;
- зависимость процессов эксплуатации АС и приложений от иностранных поставщиков или провайдеров услуг;
- комбинированные источники угроз: внешние и внутренние нарушители безопасности информации, действующие в сговоре.

5.6. Наибольшими возможностями для нанесения ущерба персональным данным, обрабатываемым организацией, обладают ее собственные работники. В этом случае содержанием деятельности нарушителя является прямое нецелевое использование предоставленных прав физического и (или) логического доступа. При этом он будет стремиться к сокрытию следов своей деятельности.

5.7. Внешний нарушитель безопасности информации, как правило, имеет сообщника (сообщников) внутри организации. При условии должного соблюдения требований к защите информации, в том числе требований к содержанию базового состава, составу мер защиты информации, установленных настоящим стандартом, соблюдения принципа "знать своего работника", реализация угроз внешними нарушителями безопасности информации, действующими самостоятельно, без соучастников внутри организации, значительно затруднена.

5.8. Выбор и применение организацией мер защиты персональных данных включает:

- выбор мер защиты персональных данных;
- адаптацию (уточнение) при необходимости выбранного состава и содержания мер защиты персональных данных с учетом модели угроз и нарушителей безопасности персональных данных организации и структурно-функциональных характеристик объектов информатизации, в том числе АС, включаемых в область применения настоящей Базовой модели;
- исключение из базового состава мер, не связанных с используемыми информационными технологиями;
- дополнение при необходимости адаптированного (уточненного) состава и содержания мер защиты персональных данных мерами, обеспечивающими выполнение требований к защите информации, установленных нормативными правовыми актами в области обеспечения безопасности и защиты персональных данных;
- применение для конкретной области адаптированного (уточненного) и дополненного состава мер защиты персональных данных.

5.9. При невозможности технической реализации отдельных выбранных мер защиты персональных данных, а также с учетом экономической целесообразности на этапах адаптации (уточнения) базового состава мер могут разрабатываться иные (компенсирующие) меры, направленные на нейтрализацию угроз безопасности персональных данных, определенных в модели угроз, и нарушителей безопасности персональных данных организации.

В этом случае организацией должно быть проведено обоснование применения компенсирующих мер защиты персональных данных.

Применение компенсирующих мер защиты персональных данных должно быть направлено на

обработку операционного риска, связанного с реализацией тех же угроз безопасности информации, на нейтрализацию которых направлены меры из базового состава мер защиты персональных данных Базовой модели, не применяемые организацией в связи с невозможностью технической реализации и (или) экономической целесообразностью.

5.10. Снижение операционного риска, связанного с нарушением безопасности персональных данных, обеспечивается путем надлежащего выбора, повышения полноты и качества применения соответствующих мер защиты информации. Полнота и качество применения мер защиты персональных данных достигается планированием, реализацией, проверкой и совершенствованием системы защиты информации, осуществляемыми в рамках системы организации и управления защитой информации, а также применением мер защиты персональных данных на этапах жизненного цикла АС и приложений.

5.11. Оценка остаточного операционного риска, связанного с неполным или некачественным применением мер защиты персональных данных, входящих в систему защиты информации, осуществляется в соответствии с процедурой, определенной требованиями нормативных актов, на основе оценки показателей соответствия целям реализации системы защиты.

5.12. Уровни защиты информации:

- уровень 3 - минимальный;
- уровень 2 - стандартный;
- уровень 1 - усиленный.

5.13. В организации формируются один или несколько контуров безопасности, для которых может быть установлен разный уровень защиты персональных данных.

5.14. Уровень защиты персональных данных организации для конкретного контура безопасности устанавливается с учетом:

- вида деятельности организации, реализуемых бизнес-процессов;
- технологических процессов обработки персональных данных;
- объема операций;
- размера организации.

5.15. Организация самостоятельно определяет необходимость использования средств криптографической защиты информации (СКЗИ) при обработке персональных данных, если иное не предусмотрено федеральными законами и иными нормативными правовыми актами Российской Федерации, в том числе нормативными актами, стандартами, правилами профессиональной деятельности.

5.16. Юридические лица или индивидуальные предприниматели, привлекаемые организацией для проведения работ по обеспечению защиты информации, должны иметь лицензию на деятельность по технической защите конфиденциальной информации.

## 6. Ограничения

6.1. В целях реализации Базовой модели режим защиты согласия субъекта персональных данных на обработку его персональных данных приравнивается к режиму защиты персональных

6.2. Организация обязана обеспечивать реализацию настоящей Базовой модели при трансграничной передаче персональных данных, а также при выполнении международных договоров.

## 7. Заключительные положения

7.2. При этом нельзя не учитывать, что по мере изменения обстоятельств и технологий источники угроз и сопутствующие риски изменяются. Поэтому Базовая модель подлежит пересмотру, для чего в организации должны быть установлены и выполняться процедуры анализа результатов мониторинга угроз.

7.3. В случае отсутствия у организации потенциала, необходимого для самостоятельной доработки Базовой модели, она совершенствуется с привлечением сторонних организаций, обладающих необходимым опытом, знаниями и компетенцией.

[illegible]