ПОЛИТИКА

информационной безопасности информационных систем персональных данных Министерства здравоохранения Калининградской области и государственных медицинских организаций Калининградской области

I. ОБЩИЕ ПОЛОЖЕНИЯ

1. Политика информационной безопасности информационных систем персональных данных Министерства здравоохранения Калининградской области и государственных медицинских организаций Калининградской области (далее - Политика) разработана в целях реализации положений Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», постановления Правительства Российской Федерации от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами», постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», иных нормативных правовых актов, руководящих и методических документов по информационной безопасности.

Политика разработана в соответствии с целями, задачами и принципами обеспечения безопасности ПДн, изложенными в Концепции информационной безопасности информационных систем персональных данных Министерства здравоохранения Калининградской области и государственных медицинских организаций Калининградской области.

Настоящая Политика  определяет:

- основные цели и задачи построения системы защиты персональных данных от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, а также для минимизации ущерба от возможной реализации угроз безопасности ПДн (далее - УБПДн);

- уровень доступа и права пользователей ИСПДн;

- требования к персоналу ИСПДн, а также степень его ответственности.

2. Действие Политики распространяется на всех государственных гражданских служащих (служащих) Министерства и сотрудников медицинских организаций (штатных, временных, работающих по трудовому договору, по контракту и других), эксплуатирующих технические и программные средства ИСПДн, на сотрудников подразделений, осуществляющих сопровождение, обслуживание и обеспечение нормального функционирования ИСПДн, а также на всех прочих лиц (подрядчики, аудиторы и т.п.).

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

В ИСПДн обеспечивается доступность авторизованных пользователей к ПДн и связанным с ними ресурсам, осуществляется своевременное обнаружение и реагирование на УБПДн, а также предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

Состав объектов защиты указывается в Перечне ПДн, обрабатываемых в связи с реализацией трудовых отношений, а также в связи с оказанием государственных услуг и осуществлением государственных функций, а также в Перечне ИСПДн.

Состав ИСПДн подлежащих защите, формируется по результатам проверки условий обработки ПДн и указывается в Отчёте.

II. СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

4. Система защиты персональных данных строится в порядке, указанном в разделе IV Концепции.

На  основании Отчета по результатам проверки условий обработки ПДн в Министерстве и в медицинских организациях, Переченя ИСПДн,  Перечня ПДн, обрабатываемых в связи с реализацией трудовых отношений, а также в связи с оказанием государственных услуг и осуществлением государственных функций, Акта классификации ИСПДн и установления уровня защищенности ПДн, Частной модели угроз безопасности ПДн при их обработке в ИСПДн; руководящих документов ФСТЭК и ФСБ России определяется необходимый уровень защищенности ПДн для каждой ИСПДн Министерства и медицинских организаций.

На основании анализа актуальных угроз безопасности ПДн, описанных в Частной модели угроз безопасности ПДн при их обработке в ИСПДн и Отчете по результатам проверки условий обработки ПДн, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн.

Выбранные необходимые мероприятия отражаются в Плане мероприятий по обеспечению защиты ПДн.

5. Для каждой ИСПДн составляется список используемых технических средств защиты, а так же программного обеспечения, участвующего в обработке ПДн во всех элементах ИСПДн:

- в автоматизированных рабочих местах пользователей;

- в серверах приложений;

- в системах управления базами данных;

- на границах локальных вычислительных сетей;

- в каналах передачи данных в сети общего пользования и (или) международного обмена, если по ним передаются ПДн.

В список используемых технических средств защиты информации также включаются функции защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами, прикладным программным обеспечением и специальными комплексами, реализующими средства защиты.

Список функций защиты включает:

- управление и разграничение доступа пользователей;

- регистрацию и учет действий с информацией;

- обеспечение целостности данных;

- обнаружение вторжений.

6. В зависимости от уровня защищенности ПДн и актуальности угроз, СЗПДн может включать следующие технические средства:

- антивирусные средства для рабочих станций пользователей и серверов;

- средства межсетевого экранирования;

- средства криптографической защиты информации при передаче защищаемой информации по каналам связи.

7. В медицинских организациях список используемых технических средств защиты информации вносится в План мероприятий по обеспечению защиты ПДн, а также в Перечень по учету применяемых средств защиты информации, эксплуатационной и технической документации к ним.

Список используемых технических средств поддерживается в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн соответствующие изменения вносятся в План мероприятий по обеспечению защиты ПДн и в Перечень по учету применяемых средств защиты информации, эксплуатационной и технической документации к ним.

Ответственность за поддержание в актуальном состоянии используемых технических средств защиты информации в ИСПДн возлагается:

- в Министерстве – заместителя министра или ответственного за организацию обработки ПДн;

- в медицинской организации - на главного врача (директора) медицинской организации или ответственного за организацию обработки ПДн.

III. ТРЕБОВАНИЯ К ПОДСИСТЕМАМ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

8. СЗПДн включает в себя следующие подсистемы:

- управления доступом, регистрации и учета;

- обеспечения целостности и доступности;

- антивирусной защиты;

- межсетевого экранирования;

- анализа защищенности;

- обнаружения вторжений;

- криптографической защиты.

Подсистемы СЗПДн имеют различные функциональные возможности в зависимости от класса ИСПДн и установленного уровня защищенности ПДн, определенных в Акте классификации ИСПДн и установления уровня защищенности ПДн.

Список соответствия функций подсистем СЗПДн классу защищенности указан в приложении к настоящей Политике.

Перечень требований, необходимых для обеспечения заданного  уровня защищенности ПДн, приведен в пункте 23 Концепции.

9. Подсистема управления доступом, регистрации и учета предназначена для реализации следующих функций безопасности:

- идентификация и проверка подлинности субъектов доступа при входе в ИСПДн;

- идентификация   терминалов,   узлов   сети,    каналов   связи,    внешних устройств по логическим именам;

- идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;

- регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее останова;

- регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;

- регистрация попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей.

Подсистема управления доступом реализуется с помощью штатных средств обработки ПДн (операционных систем, приложений, систем управления базами данных и другими программными средствами), а также с использованием специальных технических средств или их комплексов, обеспечивающих дополнительные меры по аутентификации и контролю. Например, применение единых хранилищ учетных записей пользователей и регистрационной информации, использование биометрических и технических (с помощью электронных пропусков) мер аутентификации и других.

10. Подсистема обеспечения целостности и доступности предназначена для обеспечения целостности и доступности ПДн, программных и аппаратных средств ИСПДн, а также средств защиты при случайной или намеренной их модификации.

Подсистема реализуется с помощью организации резервного копирования обрабатываемых данных, а также резервированием ключевых элементов ИСПДн.

11. Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и автоматизированных рабочих мест  пользователей ИСПДн.

Средства антивирусной защиты предназначены для реализации следующих функций:

- резидентный антивирусный мониторинг;

- антивирусное сканирование;

- скрипт-блокирование;

- централизованная           (удаленная)         установка         (деинсталляция) антивирусного программного обеспечения, настройка, администрирование, просмотр отчетов и статистической информации по работе средств антивирусной защиты;

- автоматизированное обновление антивирусных баз;

- ограничение  прав  пользователя  на  остановку   исполняемых   задач   и изменение настроек антивирусного программного обеспечения;

- автоматический запуск средств антивирусной защиты после загрузки операционной системы.

Подсистема реализуется путем внедрения антивирусного программного обеспечения во все элементы ИСПДн.

12. Подсистема межсетевого экранирования предназначена для реализации следующих функций:

- фильтрация открытого и зашифрованного (закрытого) IP-трафика по заданным параметрам;

- фиксация во внутренних журналах информации о проходящем открытом и закрытом IP-трафике;

- идентификация и аутентификация администратора межсетевого экрана при его локальных запросах на доступ;

- регистрация входа (выхода) администратора межсетевого экрана в систему (из системы) либо загрузка и инициализация системы и ее программного останова;

- контроль целостности своей программной и информационной части;

- фильтрация пакетов служебных протоколов, служащих для диагностики и управления работой сетевых устройств;

- фильтрация с учетом входного и выходного сетевого интерфейса как средства проверки подлинности сетевых адресов;

- регистрация и учет запрашиваемых сервисов прикладного уровня;

- блокирование доступа неидентифицированного объекта или субъекта, подлинность которого при аутентификации не подтвердилась, методами, устойчивыми к перехвату;

- контроль сетевой активности приложений и обнаружение сетевых атак.

Подсистема реализуется внедрением программно-аппаратных комплексов межсетевого экранирования на границе локальных вычислительных сетей для ИСПДн классов 1, 2 и 3.

13. Подсистема анализа защищенности предназначена для выявления уязвимостей, связанных с ошибками в конфигурации программного обеспечения ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему.

Функциональные возможности подсистемы реализуется программными и программно-аппаратными средствами.

14. Подсистема обнаружения вторжений обеспечивает выявление сетевых атак на элементы ИСПДн, подключенные к сетям общего пользования и (или) международного обмена.

Функциональные возможности подсистемы реализуются программными и программно-аппаратными средствами.

15. Подсистема криптографической защиты предназначена для исключения несанкционированного доступа к защищаемой информации в ИСПДн при ее передаче по каналам связи сетей общего пользования и (или) международного обмена.

Подсистема реализуется путём внедрения в ИСПДн криптографических программно-аппаратных комплексов.

IV. ПОЛЬЗОВАТЕЛИ ИНФОРМАЦИОННЫХ СИСТЕМ

ПЕРСОНАЛЬНЫХ ДАННЫХ

16. В Концепции определены основные категории пользователей ИСПДн:

- администратор;

- программист-разработчик;

- оператор.

На основании этих категорий устанавливаются группы пользователей ИСПДн и определяется их уровень доступа и полномочий.

17. Группы пользователей ИСПДн.

В ИСПДн Министерства и медицинских организаций выделяются следующие группы пользователей, участвующих в обработке ПДн:

- администратор ИСПДн;

- администратор безопасности;

- оператор автоматизированного рабочего места (далее – АРМ);

- администратор сети;

- технический      специалист        по       обслуживанию      периферийного оборудования;

- программист-разработчик ИСПДн.

Данные о типах пользователей, уровне их доступа и информированности  указываются в Отчете по результатам проверки условий обработки ПДн медицинской организации.

18. Администратор ИСПДн – государственный гражданский служащий (служащий)  Министерства, сотрудник медицинской организации, сотрудник другой организации, ответственный за настройку, внедрение и сопровождение ИСПДн. Администратор ИСПДн обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (оператора АРМ) к элементам, хранящим ПДн.

Администратор ИСПДн обладает следующим уровнем доступа и знаний:

- обладает полной информацией о системном и прикладном программном обеспечении ИСПДн;

- обладает полной информацией о технических средствах и конфигурации ИСПДн;

- имеет доступ ко всем техническим средствам обработки информации и данным ИСПДн;

- обладает правами конфигурирования и административной настройки технических средств ИСПДн.

19. Администратор безопасности - государственный гражданский служащий (служащий)  Министерства, сотрудник медицинской организации, ответственный за функционирование СЗПДн, включая обслуживание и настройку административной, серверной и клиентской части программ.

Администратор безопасности обладает следующим уровнем доступа и знаний:

- обладает правами Администратора ИСПДн;

- обладает полной информацией об ИСПДн;

- имеет доступ к средствам защиты информации и протоколирования, а также к части ключевых элементов ИСПДн;

- не имеет прав доступа к конфигурированию технических средств сети за исключением контрольных (инспекционных).

Администратор безопасности уполномочен:

- реализовывать политики безопасности в части настройки системы криптографической защиты информации, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь (оператор АРМ) получает возможность работать с элементами ИСПДн;

- осуществлять настройки системы разграничения доступа к ПДн;

- осуществлять аудит средств защиты;

- устанавливать доверительные отношения своей защищенной сети с сетями других организаций, системой межведомственного электронного взаимодействия, взаимодействующими информационными системами.

20. Оператор АРМ - государственный гражданский служащий (служащий)  Министерства, сотрудник медицинской организации, осуществляющий обработку ПДн.  Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в ИСПДн,  формирование справок и отчетов по информации, полученной из ИСПД. Оператор не имеет полномочий на управление подсистемами обработки данных и СЗПДн.

Оператор ИСПДн обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству ПДн;

- располагает конфиденциальными данными, к которым имеет доступ.

21. Администратор сети - государственный гражданский служащий (служащий)  Министерства, сотрудник медицинской организации, сотрудник другой организации, ответственный за функционирование телекоммуникационной подсистемы ИСПДн. Администратор сети не имеет полномочий на управление подсистемами обработки данных и безопасности.

Администратор сети обладает следующим уровнем доступа и знаний:

- обладает частью информации о системном и прикладном программном обеспечении ИСПДн;

- обладает частью информации о технических средствах и конфигурации ИСПДн;

- имеет физический доступ к техническим средствам обработки информации и средствам защиты;

- знает, по меньшей мере, одно легальное имя доступа.

22. Технический специалист по обслуживанию - сотрудник медицинской организации, сотрудник другой организации, который осуществляет обслуживание и настройку периферийного оборудования ИСПДн. Технический специалист по обслуживанию не имеет доступа к ПДн, не имеет полномочий на управление подсистемами обработки данных и безопасности.

Технический специалист по обслуживанию обладает следующим уровнем доступа и знаний:

- обладает частью информации о системном и прикладном программном обеспечении ИСПДн;

- обладает частью информации о технических средствах и конфигурации ИСПДн;

- знает, по меньшей мере, одно легальное имя доступа.

23. Программист- разработчик (поставщик) прикладного программного обеспечения – сотрудник медицинской организации, сотрудник другой организации,  обеспечивающий сопровождение прикладного программного обеспечения на защищаемом объекте.

Программист-разработчик (поставщик) прикладного программного обеспечения:

- обладает информацией об алгоритмах и программах обработки информации на ИСПДн;

- обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;

- может располагать любыми фрагментами информации о топологии ИСПДн и технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн.

24. На основании Отчёта по результатам проведения ежегодной проверки условий обработки ПДн администратором безопасности ИСПДн определяются права доступа к элементам ИСПДн для всех групп пользователей (настройка системы разграничения доступа к ПДн) и вносятся в Правила обработки ПДн.

V. ТРЕБОВАНИЯ К ПЕРСОНАЛУ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

25. Все государственные гражданские служащие (служащие)  Министерства, сотрудники медицинских организаций, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

При вступлении нового государственного гражданского служащего (служащего)  Министерства в должность начальник отдела правовой и кадровой работы обязан организовать его ознакомление с документами, регламентирующими требования по защите ПДн, а заместитель министра или ответственный за организацию обработки ПДн обязаны провести инструктаж по выполнению процедур, необходимых для санкционированного использования ИСПДн.

Государственные гражданские служащие (служащие) Министерства, сотрудники медицинских организаций должны быть ознакомлены с Концепцией и настоящей Политикой, а также с принятыми процедурами работы с элементами ИСПДн и СЗПДн.

26. Государственные гражданские служащие (служащие) Министерства, сотрудники медицинских организаций, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать несанкционированного доступа к ним, а также возможности их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

27. Государственные гражданские служащие (служащие) Министерства, сотрудники медицинских организаций должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

28. Государственные гражданские служащие (служащие) Министерства, сотрудники медицинских организаций 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 ПДн и процедуры защиты оборудования, оставленного без присмотра, свои обязанности по обеспечению такой защиты, а также требования Порядка доступа служащих Министерства в помещения, в которых ведётся обработка ПДн.

29. Государственным гражданским служащим (служащим) Министерства, сотрудникам медицинских организаций  запрещается:

- устанавливать постороннее программное обеспечение;

- подключать личные мобильные устройства и носители информации, записывать на них защищаемую информацию;

- хранить защищаемую информацию и ПДн на внешних ресурсах, идентифицировать физическое размещение которых не представляется возможным;

- использовать «облачные технологии» Saas, реализованные с использованием  технических и программных средств, не имеющих аттестата соответствия по требованиям безопасности информации для соответствующего класса ИСПДн.

30. Установка, удаление, обновление программного обеспечения в Министерстве, медицинских организациях осуществляется только государственными гражданскими служащими (служащими) Министерства, сотрудниками медицинских организаций или сотрудниками сторонних организаций, с которыми заключено Соглашение (договор) о конфиденциальности, либо Соглашение (договор) о соблюдении режима безопасности ПДн при выполнении работ в ИСПДн.

Государственным гражданским служащим (служащим) Министерства, сотрудникам медицинских организаций  запрещается разглашать защищаемую информацию, которая стала им известна при работе с ИСПДн, третьим лицам.

31. При работе с ПДн в ИСПДн государственные гражданские служащие (служащие) Министерства, сотрудники медицинских организаций обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов автоматизированных рабочих мест или терминалов.

При завершении работы с ИСПДн государственные гражданские служащие (служащие) Министерства, сотрудники медицинских организаций  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.

32. Государственные гражданские служащие (служащие) Министерства, сотрудники медицинских организаций  должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение.

Государственные гражданские служащие Министерства должны быть ознакомлены с Типовым обязательством государственного гражданского служащего, непосредственно осуществляющего обработку ПДн, в случае расторжения с ним трудового договора прекратить обработку ПДн, ставших известными в связи с исполнением должностных  обязанностей.

33. Государственные гражданские служащие (служащие) Министерства, сотрудники медицинских организаций  обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, которые могут повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, заместителю Министра, главному врачу (директору) медицинской организации или и (или) ответственному за организацию обработки ПДн.

34. Должностные обязанности пользователей ИСПДн указываются в следующих документах:

- Должностная инструкция ответственного за организацию обработки ПДн в Министерстве, медицинской организации;

- Типовое обязательство государственного гражданского служащего, непосредственно осуществляющего обработку ПДн, в случае расторжения с ним трудового договора прекратить обработку ПДн, ставших известными в связи с исполнением должностных  обязанностей;

- Инструкция администратора ИСПДн (при наличии);

- Инструкция администратора безопасности ИСПДн (при наличии);

- Инструкция пользователя ИСПДН (при наличии);

- Инструкция пользователя при возникновении внештатных ситуаций (при наличии).

VI. ОТВЕТСТВЕННОСТЬ СОТРУДНИКОВ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

35. В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» лица, виновные в нарушении требований данного Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность.

36. Администратор ИСПДн и администратор безопасности информации несут ответственность за все действия, совершенные от имени их учетных записей или системных учетных записей, если не доказан факт несанкционированного использования учетных записей.

37. При нарушениях правил, связанных с безопасностью ПДн, государственные гражданские служащие (служащие) Министерства, сотрудники медицинских организаций  – пользователи ИСПДн  несут ответственность, установленную действующим законодательством Российской Федерации.

38. Требования нормативных правовых актов по защите информации, а также ответственность руководителей, государственных гражданских служащих (служащих) Министерства, сотрудников медицинских организаций  за разглашение и несанкционированную модификацию (искажение, фальсификацию) ПДн, а также за неправомерное вмешательство в процессы их автоматизированной обработки указываются в Положениях о структурных подразделениях Министерства, Уставах медицинских организаций, осуществляющих обработку ПДн в ИСПДн, и в должностных регламентах (инструкциях) государственных гражданских служащих Министерства сотрудников медицинских организаций.

Приложение

к Политике информационной безопасности информационных систем персональных данных городского округа  Министерства здравоохранения Калининградской области и государственных медицинских организаций Калининградской области

СПИСОК СООТВЕТСТВИЯ

функций подсистем системы защиты персональных данных классу защищенности

информационной системы персональных данных

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| № п/п | Перечень технических мероприятий по обеспечению безопасности  информационной системы персональных данных | Класс защищённости информационной системы персональных данных | | |
| К3 | К2 | К1 |

| 1 | 2 | 3 | 4 | 5 |
| --- | --- | --- | --- | --- |
| I | В подсистеме управления доступом: |  |  |  |
| 1. | Идентификация и проверка подлинности субъектов доступа при входе в операционную систему ИСПДн по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов | + | + | + |
| 2. | Идентификация терминалов, технических средств обработки ПДн, узлов ИСПДн, компьютеров, каналов связи, внешних устройств ИСПДн по их логическим именам (адресам, номерам) | - | + | + |
| 3. | Идентификация программ, томов, каталогов, файлов, записей, полей записей по именам | - | + | + |
| 4. | Реализация контроля доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа | - | + | + |
| 5. | Реализация межсетевого экранирования при наличии подключения ИСПДн к сетям общего пользования | Не ниже 5-го уровня защищённости | Не ниже 4-го уровня защищённости | Не ниже 3-го уровня защищённости |
| 6. | Обеспечение безопасного межсетевого взаимодействия с использованием межсетевых экранов для ИСПДн  с различными классами защищённости | Не ниже 5-го уровня защищенности | Не ниже 4-го уровня защищенности | Не ниже 3-го уровня защищенности |
| II | Средство защиты от программно-математических воздействий (далее - ПМВ): |  |  |  |
| 1. | Идентификация и аутентификация субъектов доступа при входе в средство защиты от программно-математических воздействий и перед выполнением ими любых операций по управлению функциями средства защиты от ПМВ по паролю (или с использованием иного механизма аутентификации) условно-постоянного действия длиной не менее шести буквенно-цифровых символов | + | + | + |
| 2. | Осуществление контроля любых действий субъектов доступа по управлению функциями средства защиты от ПМВ только после проведения его успешной аутентификации | + | + | + |
| 3. | Наличие механизма блокирования доступа к средствам защиты от ПМВ при выполнении устанавливаемого числа неудачных попыток ввода пароля | + | + | + |
| 4. | Идентификация файлов, каталогов, программных модулей, внешних устройств, используемых средств защиты от ПМВ | + | + | + |
| III | В подсистеме регистрации и учета: |  |  |  |
| 1. | Регистрация входа (выхода) субъекта доступа в систему (из системы) либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения ИСПДн. В параметрах регистрации указываются дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы | + | + | + |
| 2. | Организация учета всех защищаемых носителей информации с помощью  маркировки и с занесением учетных данных в журнал (учетную карточку) | + | + | + |
| 3. | Регистрация входа/выхода субъектов доступа в средство защиты от ПМВ, регистрация загрузки и инициализации этого средства и ее программного останова. В параметрах регистрации указывается время и дата входа/выхода субъекта доступа в средство защиты от ПМВ или загрузки/останова этого средства, а также идентификатор субъекта доступа, инициировавшего данные действия | + | + | + |
| 4. | Регистрация событий проверки и обнаружения ПМВ. В параметрах регистрации указываются время и дата проверки или обнаружения ПМВ, идентификатор субъекта доступа, инициировавшего данные действия, характер выполняемых действий по проверке, тип обнаруженной вредоносной программы, результат действий средства защиты по блокированию ПМВ | + | + | + |
| 5. | Регистрация событий по внедрению в средство защиты от ПМВ пакетов обновлений. В параметрах регистрации указываются время и дата обновления, идентификатор субъекта доступа, инициировавшего данное действие версия и контрольная сумма пакета обновления | + | + | + |
| 6. | Регистрация событий запуска/завершения работы модулей средства защиты от ПМВ. В параметрах регистрации указываются время и дата запуска/завершения работы, идентификатор модуля, идентификатор субъекта доступа, инициировавшего данное действие, результат запуска/завершения работы | + | + | + |
| 7. | Регистрация событий управления субъектом доступа функциями средства защиты от ПМВ. В параметрах регистрации указываются время и дата события управления каждой функцией, идентификатор и спецификация функции, идентификатор субъекта доступа, инициировавшего данное действие, результат действия | + | + | + |
| 8. | Регистрация событий попыток доступа программных средств к модулям средства защиты от ПМВ или специальным ловушкам. В параметрах регистрации указываются время и дата попытки доступа, идентификатор модуля, идентификатор и спецификация модуля средства защиты от ПМВ (специальной ловушки), результат попытки доступа | + | + | + |
| 9. | Регистрация событий отката для средства защиты от ПМВ. В параметрах регистрации указываются время и дата события отката, спецификация действий отката, идентификатор субъекта доступа, инициировавшего данное действие, результат действия | + | + | + |
| 10. | Обеспечение защиты данных регистрации от их уничтожения или модификации нарушителем | + | + | + |
| 11. | Реализация механизма сохранения данных регистрации в случае сокращения отведенных под них ресурсов | + | + | + |
| 12. | Реализация механизма просмотра и анализа данных регистрации и их фильтрации по заданному набору параметров | + | + | + |
| 13. | Автоматический непрерывный мониторинг событий, которые могут являться причиной реализации ПМВ (создание, редактирование, запись, компиляция объектов, которые могут содержать вредоносные программы) | + | + | + |
| 14. | Реализация механизма автоматического анализа данных регистрации по шаблонам типовых проявлений ПМВ с автоматическим их блокированием и уведомлением администратора безопасности | + | + | + |
| 15. | Проведение нескольких видов учета (дублирующих) с регистрацией выдачи (приема) носителей информации | + | + | + |
| 16. | Регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы | - | + | + |
| 17. | Регистрация выдачи печатных (графических) документов на «твердую» копию. В параметрах регистрации указываются (дата и время выдачи (обращения к подсистеме вывода), спецификация устройства выдачи – логическое имя (номер) внешнего устройства, краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа, идентификатор субъекта доступа, запросившего документ | - | + | + |
| 18. | Регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются дата и время запуска, имя (идентификатор) программы (процесса, задания), идентификатор субъекта доступа, запросившего программу (процесс, задание), результат запуска (успешный, неуспешный – несанкционированный) | - | + | + |
| 19. | Регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются дата и время попытки доступа к защищаемому файлу с указанием ее результата (успешная, неуспешная – несанкционированная), идентификатор субъекта доступа, спецификация защищаемого файла | - | + | + |
| 20. | Регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, компьютерам, узлам сети ИСПДн, линиям (каналам) связи, внешним устройствам компьютеров, программам, томам, каталогам, файлам, записям, полям записей. В параметрах регистрации указываются дата и время попытки доступа к защищаемому объекту с указанием ее результата (успешная, неуспешная – несанкционированная), идентификатор субъекта доступа, спецификация защищаемого объекта – логическое имя (номер) | - | + | + |
| 21. | Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти компьютеров и внешних накопителей. Очистка осуществляется однократной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов, информации) | - | + | + |
| IV | В подсистеме обеспечения целостности: |  |  |  |
| 1. | Обеспечение целостности программных средств защиты в составе СЗПДн, а также неизменность программной среды. При этом целостность средств защиты проверяется при загрузке системы по наличию имен (идентификаторов) компонент СЗПДн, целостность программной среды обеспечивается отсутствием в ИСПДн средств разработки и отладки программ | + | + | + |
| 2. | Осуществление физической охраны ИСПДн (устройств и носителей информации), предусматривающее контроль доступа в помещения ИСПДн посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения ИСПДн и хранилище носителей информации | + | + | + |
| 3. | Периодическое тестирование функций СЗПДн при изменении программной среды и персонала ИСПДн с помощью тест-программ, имитирующих попытки НСД | + | + | + |
| 4. | Наличие средств восстановления СЗПДн, предусматривающих ведение двух копий программных средств защиты информации, их периодическое обновление и контроль работоспособности | + | + | + |
| 5. | Проверка целостности модулей средства защиты от ПМВ, необходимых для его корректного функционирования, при его загрузке с использованием контрольных сумм | + | + | + |
| 6. | Восстановление средств защиты от ПМВ, предусматривающее ведение двух копий программных средств защиты, их периодическое обновление и контроль работоспособности | + | + | + |
| 7. | Реализация механизма проверки целостности пакетов обновлений средства защиты от ПМВ с использованием контрольных сумм | + | + | + |
| 8. | Резервное копирование ПДн на отчуждаемые носители информации | - | + | + |
| V | В подсистеме антивирусной защиты: |  |  |  |
| 1. | Автоматическая проверка на наличие вредоносных программ или последствий ПМВ при импорте в ИСПДн всех программных модулей (прикладных программ), которые могут содержать вредоносные программы, по их типовым шаблонам и с помощью эвристического анализа | + | + | + |
| 2. | Реализация механизма автоматического блокирования обнаруженных вредоносных программ путем их удаления из программных модулей или уничтожения | + | + | + |
| 3. | Регулярное выполнение (при первом запуске средств защиты ПДн от ПМВ и с устанавливаемой периодичностью) проверки на предмет наличия в них вредоносных программ | + | + | + |
| 4. | Автоматическое инициирование проверки ИСПДн на предмет наличия вредоносных программ при выявлении факта ПМВ | + | + | + |
| 5. | Реализация механизма отката для устанавливаемого числа операций удаления вредоносной программы из оперативной или постоянной памяти, из программных модулей и прикладных программ или программных средств, содержащих вредоносную программу | + | + | + |
| 6. | Автоматический и непрерывный мониторинг информационного обмена ИСПДн с внешней сетью с целью выявления вредоносных программ | + | + | + |
| VI | В подсистеме контроля отсутствия недекларированных возможностей в программное обеспечение средства защиты информации: |  |  |  |
| 1. | Для программного обеспечения, используемого при защите информации в ИСПДн (средств защиты информации, в том числе и встроенных в общесистемное и прикладное программное обеспечение), должен быть обеспечен соответствующий уровень контроля отсутствия в нем недекларированных возможностей | + | + | + |
| VII | Обнаружение вторжений в ИСПДн: |  |  |  |
| 1. | Использование в составе ИСПДн программных или программно-аппаратных средств (систем) обнаружения вторжений | + | + | + |
| 2. | Обязательное использование системы обнаружения сетевых атак, использующие сигнатурные методы анализа | + | - | - |
| 3. | Обязательное использование системы обнаружения сетевых атак, использующие сигнатурные методы анализа и методы выявления аномалий | - | + | + |
| VIII | Защита ИСПДн от побочных электромагнитных излучений и наводок: |  |  |  |
| 1. | Использование средств вычислительной техники для обработки информации, удовлетворяющих требованиям стандартов Российской Федерации по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам персональных электронных вычислительных машин (например, ГОСТ 29216 91, ГОСТ Р 50948-2001, ГОСТ Р 50949-2001, ГОСТ Р 50923 96, СанПиН 2.2.2.542 96) | + | + | + |
| IX | Оценка соответствия ИСПДн требованиям безопасности ПДн |  |  |  |
| 1. | Обязательная сертификация (аттестация) по требованиям безопасности информации | - | + | + |
| 2. | Декларирование соответствия или обязательная сертификация (аттестация) по требованиям безопасности информации (по решению оператора) | + | - | - |

Примечание: Для ИСПДн 4 класса защищённости перечень мероприятий по защите ПДн определяется в зависимости от ущерба, который может быть нанесен вследствие несанкционированного или непреднамеренного доступа к ПДн.