

**УТВЕРЖДАЮ**

Директор МБУ ДО ЦДТТ «Юность»

Краснов О.Л.

Приказ № 85  
от «17» декабря 2018г.



## **Политика информационной безопасности информационных систем персональных данных**

Перечень обозначений и сокращений, используемых в Политике информационной безопасности информационных систем персональных данных:

**АВС** - антивирусные средства

**АРМ** - автоматизированное рабочее место

**ИСПДн** - информационная система персональных данных

**НСД** - несанкционированный доступ

**ОС** - операционная система

**ПДн** - персональные данные

**ПО** - программное обеспечение

**СКЗИ** - средства защиты информации

**СЗПДн** - система (подсистема) защиты персональных данных

**УБПДн** - угрозы безопасности персональных данных

### **Введение**

Настоящая Политика информационной безопасности МБУ ДО ЦДТТ «Юность» (далее - Политика) является официальным документом. Политика разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» и постановления Правительства Российской Федерации от 1 ноября 20012 г. №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». В Политике определены требования к персоналу ИСПДн, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в ИСПДн школы.

### **1. Общие положения**

Целью настоящей Политики является обеспечение безопасности объектов защиты МБУ ДО ЦДТТ «Юность» от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности ПДн (УБПДн). 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 УБПДн. Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

### **2. Область действия.**

Требования настоящей Политики распространяются на всех сотрудников МБУ ДО ЦДТТ «Юность» (штатных, временных, работающих по контракту и т. п.), а также всех прочих лиц (подрядчики, аудиторы и т. п.).

### **3. Система защиты персональных данных**

Система защиты персональных данных (СЗПДн), строится на основании:

- Перечня персональных данных, подлежащих защите;
- Акта классификации информационной системы персональных данных;
- Модели угроз безопасности персональных данных.

На основании этих документов определяется необходимый уровень защищенности ПДн каждой ИСПДн МБУ ДО ЦДТТ «Юность». На основании анализа актуальных угроз безопасности ПДн, описанного в Модели угроз 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.

Для каждой ИСПДн должен быть составлен список используемых технических средств защиты, а так же программного обеспечения, участвующего в обработке ПДн, на всех элементах ИСПДн:

- АРМ пользователей;
- Каналов передачи в сети общего пользования и (или) международного обмена, если по ним передаются ПДн.

В зависимости от уровня защищенности ИСПДн и актуальных угроз, СЗПДн может включать следующие технические средства:

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

Так же в список должны быть включены функции защиты, обеспечиваемые штатными средствами обработки ПДн операционными системами (ОС), прикладным ПО и специальными комплексами, реализующими средства защиты. Список функций защиты может включать:

- управление и разграничение доступа пользователей;
- регистрацию и учет действий с информацией;
- обеспечения целостности данных;
- обнаружение вторжений.

Список используемых технических средств отражается в Плане мероприятий по обеспечению защиты персональных данных. Список используемых средств должен поддерживаться в актуальном состоянии. При изменении состава технических средств защиты или элементов ИСПДн, соответствующие изменения должны быть внесены в Список и утверждены директором МБУ ДО ЦДТТ «Юность».

**4. Требования к подсистемам системы защиты персональных данных СЗПДн** включает в себя следующие подсистемы:

- управления доступом, регистрации и учета;
- обеспечения целостности и доступности;
- антивирусной защиты;
- анализа защищенности;
- обнаружения вторжений;
- криптографической защиты.

Подсистемы СЗПДн имеют различный функционал в зависимости от класса ИСПДн, определенного в Акте классификации информационной системы персональных данных.

#### **4.1. Подсистемы управления доступом, регистрации и учета**

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

- идентификации и проверка подлинности субъектов доступа при входе в ИСПДн;
- идентификации терминалов, узлов сети, каналов связи, внешних устройств по логическим именам;
- идентификации программ, томов, каталогов, файлов, записей, полей записей по именам;
- регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее останова.
- регистрации попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам;

- регистрации попыток доступа программных средств к терминалам, каналам связи, программам, томам, каталогам, файлам, записям, полям записей. Подсистема управления доступом может быть реализована с помощью штатных средств обработки ПДн (операционных систем, приложений). Так же может быть внедрено специальное техническое средство или их комплекс, осуществляющие 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.

#### **4.2. Подсистема обеспечения целостности и доступности**

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

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

#### **4.3. Подсистема антивирусной защиты**

Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты АРМ пользователей ИСПДн.

Средства антивирусной защиты предназначены для реализации следующих функций:

- резидентный антивирусный мониторинг;
- антивирусное сканирование;
- скрипт-блокирование;
- централизованную (удаленную) установку (деинсталляцию) антивирусного продукта, настройку, администрирование, просмотр отчетов и статистической информации по работе продукта;
- автоматизированное обновление антивирусных баз;
- ограничение прав пользователя на остановку исполняемых задач и изменения настроек антивирусного программного обеспечения;
- автоматический запуск сразу после загрузки операционной системы. Подсистема реализуется путем внедрения специального антивирусного программного обеспечения на все элементы ИСПДн.

#### **4.4. Подсистема анализа защищенности**

Подсистема анализа защищенности, должна обеспечивать выявление уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн, которые могут быть использованы нарушителем для реализации атаки на систему.

Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

#### **4.5. Подсистема обнаружения вторжений**

Подсистема обнаружения вторжений, должна обеспечивать выявление сетевых атак на элементы ИСПДн подключенные к сетям общего пользования и (или) международного обмена. Функционал подсистемы может быть реализован программными и программно-аппаратными средствами.

#### **4.6. Подсистема криптографической защиты**

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

Подсистема реализуется внедрением криптографических программно-аппаратных комплексов.

### **5. Пользователи ИСПДн**

В ИСПДн учреждения можно выделить следующие группы пользователей, участвующих в обработке и хранении ПДн:

- Администратора ИСПДн;
- Администратора безопасности;

- Оператора АРМ.

### **5.1. Администратор ИСПДн**

Администратор ИСПДн - ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя (Оператора АРМ) к элементам, хранящим персональные данные. К данной группе могут относиться как сотрудники МБУ ДО ЦДТТ «Юность», так и сотрудники сторонних организаций. 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.

### **5.2. Администратор безопасности**

Администратор безопасности - ответственный за функционирование СЗПДн, включая обслуживание и настройку административной и клиентской компонент. К данной группе могут относиться как сотрудники МБУ ДО ЦДТТ «Юность», так и сотрудники сторонних организаций. 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 и к части ключевых элементов ИСПДн;
- имеет права доступа к конфигурированию технических средств сети. Администратор безопасности уполномочен:
- реализовывать политики безопасности в части настройки СКЗИ и систем обнаружения атак, в соответствии с которыми пользователь (Оператор АРМ) получает возможность работать с элементами ИСПДн;
- осуществлять аудит средств защиты;
- устанавливать доверительные отношения своей защищенной сети с сетями других Учреждений.

### **5.3. Оператор АРМ**

Оператор АРМ, сотрудник МБУ ДО ЦДТТ «Юность», осуществляющий обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчетов по информации, полученной из ИСПД. Оператор не имеет полномочий для управления 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.
6. Требования к персоналу по обеспечению защиты ПДн

Все сотрудники МБУ ДО ЦДТТ «Юность», 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 в должность нового сотрудника непосредственный заведующий отделом, в которое он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, а также обучение навыкам выполнения процедур, необходимых для санкционированного использования ИСПДн.

Сотрудник должен быть ознакомлен со сведениями настоящей Политики, принятых процедур работы с элементами ИСПДн и СЗПДн.

Сотрудники МБУ ДО ЦДТТ «Юность» должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей. Сотрудники МБУ ДО ЦДТТ «Юность» 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, а также свои обязанности по обеспечению такой защиты.

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

Сотрудникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами МБУ ДО ЦДТТ «Юность» третьим лицам. При работе с ПДн в ИСПДн сотрудники МБУ ДО ЦДТТ «Юность» обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ или терминалов. При завершении работы с ИСПДн сотрудники обязаны защитить АРМ или терминалы с помощью блокировки ключом или эквивалентного средства контроля, например, доступом по паролю, если не используются более сильные средства защиты. Сотрудники МБУ ДО ЦДТТ «Юность» должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утвержденной формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политику и процедуры безопасности ПДн. Сотрудники 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, руководству подразделения и лицу, отвечающему за безопасность ПДн.

#### **7. Должностные обязанности пользователей ИСПДн**

Должностные обязанности пользователей ИСПДн описаны в следующих документах:

- Инструкция администратора ИСПДн;
- Инструкция администратора безопасности ИСПДн;
- Инструкция пользователя ИСПДн;
- Инструкция пользователя при возникновении внештатных ситуаций.

#### **8. Ответственность сотрудников ИСПДн МБУ ДО ЦДТТ «Юность»**

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 гражданскую, уголовную, административную, дисциплинарную и иную предусмотренную законодательством Российской Федерации ответственность. Действующее законодательство РФ позволяет предъявлять требования по обеспечению безопасной работы с защищаемой информацией и предусматривает ответственность за нарушение установленных правил эксплуатации ЭВМ и систем, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы ЭВМ или сетей (статьи 272,273 и 274 УК РФ). Администратор ИСПДн и администратор 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 МБУ ДО ЦДТТ «Юность» - пользователей ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

Приведенные выше требования нормативных документов по защите информации должны быть отражены в должностных инструкциях сотрудников МБУ ДО ЦДТТ «Юность», а именно ответственность руководителей и сотрудников за разглашение и несанкционированную модификацию (искажение, фальсификацию) ПДн, а также за неправомерное вмешательство в процессы их автоматизированной обработки.

№	План - перечень технических мероприятий по обеспечении безопасности ИСПД	К2
I	<b>В подсистеме управления доступом:</b>	
1	Реализовать идентификацию и проверку подлинности субъектов доступа при входе в операционную систему ИСПДн по паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов;	+
2	Реализовать идентификацию терминалов, технических средств обработки ПДн, узлов ИСПДн, компьютеров, каналов связи, внешних устройств ИСПДн по их логическим именам (адресам, номерам);	+
3	Реализовать идентификацию программ, томов, каталогов, файлов, записей, полей записей по именам;	+
4	Реализовать контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа.	+
II	<b>Средство защиты от программно математических воздействий (ПМВ):</b>	
1	Реализовать идентификацию и аутентификацию субъектов доступа при входе в средство защиты от программно математических воздействий (ПМВ) 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.	Осуществлять контроль любых действий субъектов доступа по управлению функциями средства защиты от ПМВ только после проведения его успешной аутентификации;	+
3	Предусмотреть механизмы блокирования доступа к средствам защиты от ПМВ при выполнении устанавливаемого числа неудачных попыток ввода пароля.	+
III	<b>В подсистеме регистрации и учета:</b>	
1	Осуществлять регистрацию входа (выхода) субъекта доступа в систему (из системы), либо регистрацию 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	Проводить учет всех защищаемых носителей информации с помощью их любой маркировки и с занесением учетных данных в журнал (учетную карточку);	+
3	Проводить регистрацию входа/выхода субъектов доступа в средство защиты от ПМВ, регистрацию 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	Проводить регистрацию 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 (ВП), результат действий средства защиты по блокированию ПМВ;	+

5	Проводить регистрацию 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	Проводить регистрацию 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	должна проводиться 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	Проводить регистрацию 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	Проводить регистрацию 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	Обеспечить защиту данных регистрации от их уничтожения или модификации нарушителем;	+
11	Реализовать механизмы сохранения данных регистрации в случае сокращения отведенных под них ресурсов;	+
12	Реализовать механизмы просмотра и анализа данных регистрации и их фильтрации по заданному набору параметров;	+
13	Проводить автоматический непрерывный мониторинг событий, которые могут являться причиной реализации ПМВ (создание, редактирование, запись, компиляция объектов, которые могут содержать ВП).	+
14	Реализовать механизм автоматического анализа данных регистрации по шаблонам типовых проявлений ПМВ с автоматическим их блокированием и уведомлением администратора безопасности;	+
15	Проводить несколько видов учета (дублирующих) с регистрацией выдачи (приема) носителей информации;	+
16	Осуществлять регистрацию входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы.	+
17	Осуществлять регистрацию 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	Осуществлять регистрацию 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	Осуществлять регистрацию 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	Осуществлять регистрацию 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	Проводить учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);	+
22	Осуществлять очистку (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);	+
<b>IV</b>	<b>В подсистеме обеспечения целостности:</b>	
1	Обеспечить целостность 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	Осуществлять физическую охрану ИСПДн (устройств и носителей информации), предусматривающая контроль доступа в помещения ИСПДн посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения ИСПДн и хранилище носителей информации;	+
3	Проводить периодическое тестирование функций СЗПДн при изменении программной среды и персонала ИСПДн с помощью тест-программ, имитирующих попытки НСД;	+
4	должны быть в наличии средства восстановления СЗПДн, предусматривающие ведение двух копий программных средств защиты информации, их периодическое обновление и контроль работоспособности;	+
5	Проводить проверку целостности модулей средства защиты от ПМВ, необходимых для его корректного функционирования, при его загрузке с использованием контрольных сумм;	+
6	Обеспечить возможность восстановления средства защиты от ПМВ, предусматривающая ведение двух копий программного средств защиты, его периодическое обновление и контроль работоспособности;	+
7	Реализовать механизмы проверки целостности пакетов обновлений средства защиты от ПМВ с использованием контрольных сумм;	+



8	Проводить резервное копирование ПДн на отчуждаемые носители информации;	+
<b>V</b>	<b>В подсистеме антивирусной защиты:</b>	
1	Проводить автоматическую проверку на наличие ВП или последствий ПМВ при импорте в ИСПДн всех программных модулей (прикладных программ), которые могут содержать ВП, по их типовым шаблонам и с помощью эвристического анализа;	+
2	Реализовать механизмы автоматического блокирования обнаруженных ВП путем их удаления из программных модулей или уничтожения;	+
3	Регулярно выполнять (при первом запуске средств защиты ПДн от ПМВ и с устанавливаемой периодичностью) проверка на предмет наличия в них ВП;	+
4	Должна инициироваться автоматическая проверка ИСПДн на предмет наличия ВП при выявлении факта ПМВ;	+
5	Реализовать механизм отката для устанавливаемого числа операций удаления ВП из оперативной или постоянной памяти, из программных модулей и прикладных программ или программных средств, содержащих ВП.	+
6	Дополнительно в ИСПДн должен проводиться непрерывный автоматический мониторинг информационного обмена с внешней сетью с целью выявления ВП.	+
<b>VI</b>	<b>Контроль отсутствия НДВ в ПО СЗИ</b>	
1	Для программного обеспечения, используемого при защите информации в ИСПДн (средств защиты информации - СЗИ, в том числе и встроенных в общесистемное и прикладное программное обеспечение - ПО), должен быть обеспечен соответствующий уровень контроля отсутствия в нем НДВ (не декларированных возможностей).	+
<b>VII</b>	<b>Обнаружение вторжений в ИСПДн</b>	
	Обнаружение вторжений должно обеспечиваться путем использования в составе ИСПДн программных или программно-аппаратных средств (систем) обнаружения вторжений (СОВ).	*
<b>VIII</b>	<b>Защита ИСПДн от ПЭМИН</b>	
1	Для обработки информации необходимо использовать СВТ, удовлетворяющие требованиям стандартов Российской Федерации по электромагнитной совместимости, по безопасности и эргономическим требованиям к средствам отображения информации, по санитарным нормам, предъявляемым к видеодисплейным терминалам ПЭВМ (например, ГОСТ 29216 91, ГОСТ Р 50948- 2001, ГОСТ Р 50949-2001, ГОСТ Р 50923 96, СанПиН 2.2.2.542 96).	+
<b>IX</b>	<b>Оценка соответствия ИСПДн требованиям безопасности ПДн</b>	
1	Декларировать соответствие по требованиям безопасности информации (по решению оператора);	+