

Приложение 4  
к приказу МКДОВ ДС № 19  
«Красная шапочка» с.Шведино  
от 18.08.2014 г. № 28

«Утверждаю»  
Заведующий МКДОВ ДС № 19  
«Красная шапочка» с.Шведино  
Т.А.Токарева



Е.В.Товкань

«Согласовано»  
Председатель ПК  
*[Signature]*

Политика информационной безопасности  
муниципального казенного образовательного учреждения  
детский сад № 19 «Красная шапочка» с.Шведино

Термины и определения

В настоящем документе используются следующие термины и их определения.

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая

информационную технологию выполнения установленных функций.

Аутентификация отправка данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами

несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и

самовоспроизведению.

Внешняя информационная система – информационная система, взаимодействующая с информационной системой оператора из-за пределов

границ информационной системы оператора.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информацию или ресурсы информационной системы.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения информации, устанавливаемые совместно с техническими средствами и

системами, предназначенными для обработки информации или в помещениях, в которых установлены информационные системы.

Государственные информационные системы – системы – федеральные информационные системы и региональные информационные системы, созданные на основании соответствующих законов, законов

субъектов Российской Федерации, на основании правовых актов государственных органов.

Доступ в операционную среду компьютера – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступность информации – свойство безопасности информации, при котором субъекты доступа, имеющие права доступа, могут беспрепятственно их реализовать.

Защита доступа – элемент средства информации, скрытно вносимый (заглаживаемый или вносимый) в места возможного съема информации (в том числе в отражение, конструкцию, оборудование, предметы интерфейса, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация – информация, выявляющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованийми, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам доступа, объектам доступа и идентификаторов (уникальных имен) и (или) сравнение представляемого идентификатора с перечнем присвоенных идентификаторов.

Идентифицируемые и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация, обрабатываемая в информационной системе.

Информационная система – совокупность содержащихся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Информация ограничена – информация, доступ к которой ограничен федеральными законами.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона – пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, а также транспортных, технических или иных средств.

Конфиденциальность информации – свойство безопасности информации, при котором доступ к ней осуществляется только субъекты доступа, имеющие на него право.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программно-аппаратное (средство (комплекс),

реализующее контроль за информацией, поступающей в информационную систему и (или) выходящей из информационной системы.

Недекларированные возможности – функции, возможности, не описанные в описании средств вычислительной техники, не описанные или не соответствующие описанным в документе, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами.

Носитель информации – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит своё отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Общедоступная информация – это общезвестные сведения и иная информация, доступ к которой не ограничен.

Оператор информационной системы – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

Техническое средство – аппаратное или программно-аппаратное устройство, осуществляющее формирование, обработку, передачу или прием информации в информационной системе.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информационных сигналов.

Персональные данные – любая информация, относящаяся к определенному или определяемому на основании такой информации к физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.

Подочные электроматричные изучения и наводки – электроматричные изучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электроматричные наводки этих сигналов на тоководящие линии, конструкции и цепи питания.

Политика «чистого стола» – комплекс организационных мероприятий, контролируемых отсутствием записывания на бумажные носители ключей и атрибутов доступа (паролей) и хранения их вблизи объектов доступа.

Пользователь – лицо, которому разрешено выполнять некоторые действия (операции) по обработке информации в информационной системе или использующее ресурсы ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа к объектам доступа.

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информации системы и (или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие – воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Ресурс информационной системы – имеющийся элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (объект) – пользователь, процесс, выполняющие операции (действия) над объектами доступа и действия которых регламентируются правилами разграничения доступа.

Технический канал утечки информации – совокупность носителей информации (средства обработки), физической среды распространения информации вычислительного сигнала и средств, которыми добывается защищаемая информация.

Уязвимость – слабая в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – свойство безопасности информации, при котором отсутствует любое ее изменение либо изменение субъектами доступа, имеющими на него право.

### Обозначения и сокращения

- АРМ автоматизированное рабочее место
- ГИС государственная информационная система
- ЛВС локальная вычислительная сеть
- МЭ межсетевой экран
- НСД несанкционированный доступ
- ОС операционная система
- ПМВ программно-математическое воздействие
- ПДн персональные данные
- ПЭМИН побочные электромагнитные излучения и наводки
- ПО программное обеспечение
- СЗИДн система (подсистема) защиты персональных данных
- СОВ система обнаружения вторжений
- УБИОД угрозы безопасности информации от раннего доступа

### Введение

Настоящая Политика информационной безопасности (далее – Политика) разработана в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановления Правительства Российской Федерации от 21 марта 2012 г. № 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, выполняющими государственные или муниципальными органами» и приказа ФСТЭК № 17 от 11 февраля 2013 г. «Об утверждении требований к персоналу ИСПДн, степени защищенности персонала, структура и необходимый уровень ответственности ИСПДн, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности ИСПДн.

Целью настоящей Политики является обеспечение безопасности объектов защиты ИСПДн от всех видов угроз, внешних и внутренних, умышленных и не преднамеренных, минимизация ущерба от возможной реализации угроз безопасности информации (далее – УБИ). Безопасность информации достигается путем исключения несанкционированного, в том числе случайного, доступа к информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение информации, а также иных несанкционированных действий. Информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБИ. Должно осуществляться предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций, или уничтожений данных.

### 1. Общие положения

Настоящая Политика информационной безопасности (далее – Политика) разработана в соответствии с целями, задачами и принципами обеспечения безопасности информации ИСПДн, изложенными в Концепции информационной безопасности (далее – Концепция), составленной государственными органами (далее – Государственный орган), составляющие государственную тайну (далее – Государственная тайна), в соответствии с требованиями Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановления Правительства Российской Федерации от 21 марта 2012 г. № 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, выполняющими государственные или муниципальными органами» и приказа ФСТЭК № 17 от 11 февраля 2013 г. «Об утверждении требований к персоналу ИСПДн, степени защищенности персонала, структура и необходимый уровень ответственности ИСПДн, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности ИСПДн.

## 2. Область действия

Требования настоящей Политики распространяются на всех сотрудников ДЮУ (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (подрядчики, аудиторы и т.п.).

### 3. Система защиты информации

Система защиты персональных данных (далее – СЗИДн) строится на основании:

- Отчета о результатах обследования ДЮУ в части выполнения требований законодательства Российской Федерации по вопросам обеспечения информации информационных системах;
- Перечень информационных систем персональных данных в ДЮУ;
- Положений о разграничении прав доступа к обрабатываемой информации ограниченного доступа;
- Рукководящих документов ФСТЭК и ФСБ России.

На основании этих документов определяется необходимый уровень значимости информации, обрабатываемой в СЗИДн. На основании анализа актуальных угроз безопасности информации, описанных в Отчете о результатах обследования СЗИДн, делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности информации.

Для СЗИДн должен быть составлен перечень используемых технических средств, а также программного обеспечения участвующего в обработке информации, на всех элементах СЗИДн:

- АРМ пользователей;
- серверы приложений;
- СУБД;
- граница ЛВС;

- каналов передачи в сети общего пользования и (или) международного обмена, если по ним передается защищаемая информация.

В зависимости от класса защищенности СЗИДн и актуальных угроз, СЗИДн может включать следующие технические средства защиты информации:

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

Так же в перечень должны быть включены функции защиты, обеспечиваемые штатными средствами обработки защищаемой информации ОС, прикладным ПО и специальными комплексами, реализующими средства защиты. Список функций защиты может включать:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;

- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
  - защиту машинных носителей информации;
  - регистрацию событий безопасности;
  - активную защиту;
  - обнаружение (предотвращение) вторжений;
  - контроль (анализ) защищенности информации;
  - целостность информации и информации;
  - доступность информации;
  - защиту среды виртуализации;
  - защиту технических средств;
  - защиту информации и передачи данных.

#### 4. Требования к подсистемам СЭПД

СЭПД может включать в себя следующие подсистемы:

- идентификацию и аутентификацию субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защиту машинных носителей информации;
- регистрацию событий безопасности;
- активную защиту;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности информации;
- целостность информации и информации;
- доступность информации;
- защиту среды виртуализации;
- защиту технических средств;
- защиту информации и передачи данных.

Подсистемы СЭПД имеют различный функционал в зависимости от класса защищенности, определенного в Акте классификации для СЭПД.

#### 5. Пользователи СЭПД

В Концепции информационной безопасности определены основные категории пользователей. На основании этих категорий должна быть произведена типизация пользователей СЭПД, определен их уровень доступа и возможности.

В СЭПД можно выделить следующие группы пользователей, участвующих в обработке и хранении защищаемой информации:

- Администратор;
- Администратор безопасности;
- Оператор АРМ;
- Администратор сети;

- Технический специалист по обслуживанию периферийного оборудования;

- Программист-разработчик ИСПДн.

Данные о группах пользователей, уровне их доступа и информированности должны быть отражены в «Логическом описании прав доступа к обрабатываемой информации ограниченного доступа».

### 5.1 Администратор ИСПДн

Администратор – штатный сотрудник, ответственный за настройку, внедрение и сопровождение ИСПДн. Обеспечивает функционирование подсистемы управления доступом ИСПДн и полномочен осуществлять предоставление и разграничение доступа конечного пользователя (Оператора АРМ) к элементам, хранящим информацию.

Администратор 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 ИСПДн;

- обладает правами конфигурирования и административной настройки технических средств ИСПДн.

### 5.2 Администратор безопасности

Администратор безопасности – штатный сотрудник, ответственный за функционирование СЭПДн включая обслуживание и настройку административной, серверной и клиентской компонент.

знаний:

- обладает правами Администратора ИСПДн;

- обладает полной информацией об ИСПДн;

- имеет доступ к средствам защиты информации и протоколирования и 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 СКЗИ,

межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь (Оператор АРМ) получает возможность работать с элементами ИСПДн;

- осуществлять аудит средств защиты.

### 5.3 Оператор АРМ

Оператор АРМ, сотрудник, осуществляющий обработку информации. Обработка информации включает: просмотр, ручной ввод в систему, формирование справок и отчетов по информации, полученной из ИСПДн. Оператор не имеет полномочий для управления подсистемами обработки данных и СЭПДн.



Оператор ИСПДн обладает следующим уровнем доступа и знаний:  
- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству защищаемой информации;

5.4 Администратор сети  
- располагает конфиденциальными данными, к которым имеет доступ.  
Администратор сети - штатный сотрудник, ответственный за функционирование телекоммуникационной подсистемы ИСПДн. Администратор сети не имеет полномочий для управления подсистемами обработки данных и безопасности.  
Администратор сети обладает следующим уровнем доступа и знаний:  
- обладает частью информации о конфигурации ИСПДн;

- обладает частью информации о технических средствах и конфигурации ИСПДн;  
- имеет физический доступ к техническим средствам обработки информации и средствам защиты;

5.5 Технический специалист по обслуживанию периферийного оборудования  
- знает, по меньшей мере, одно легальное имя доступа.  
Технический специалист по обслуживанию периферийного оборудования, осуществляющий обслуживание и настройку периферийного оборудования ИСПДн. Технический специалист по обслуживанию не имеет доступа к защищаемой информации, не имеет полномочий для управления 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;

Лицо этой категории:  
- обладает информацией об алгоритмах и программах обработки информации в ИСПДн;  
- обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИСПДн на стадии ее разработки, внедрения и сопровождения;  
- знает, по меньшей мере, одно легальное имя доступа.  
5.6 Программист-разработчик ИСПДн  
Программисты-разработчики (поставщики) прикладного программного обеспечения - лица, обеспечивающие его сопровождение на защищаемом объекте. К данной группе относятся как штатные сотрудники, так и сторонние организации.

Лицо этой категории:  
- обладает информацией об алгоритмах и программах обработки информации в 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 информации, 6. Требования к персоналу по обеспечению защиты информации знать и строго выполнять установленные правила и обязанности по доступу к ИСПДн.

При вступлении в должность нового сотрудника непосредственный начальник подразделения, в котором он поступает, обязан организовать его ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите информации, а также обучение навыкам выполнения процедур, необходимых для санкционирования использования ИСПДн.

Сотрудник должен быть ознакомлен со сведениями настоящей Политики, приняты процедуры работы с элементами ИСПДн и СЭПДн. Сотрудники, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать ИСПДн к ним, а также возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Сотрудники должны следовать установленным процедурам поддержания режима безопасности информации при выборе и использовании паролей (если не используются технические средства аутентификации). Сотрудники должны обеспечивать надежность защиты оборудования, особенно в тех случаях, когда в помещении остаются без присмотра, обязаны знать требования оборудования и процедуры защиты оборудования, а также записывать на них защищаемую информацию, которая стала им известна при работе с информационными системами, третьим лицам.

При работе с защищаемой информацией в ИСПДн сотрудники обязаны обеспечить отсутствие возможности просмотра информации 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 должны быть проинформированы об угрозах нарушения режима безопасности информации и ответственности за его нарушение. Они

должны быть ознакомлены с утвержденной формальной процедурой принятия политики и процедуры безопасности Информации, которые нарушили наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые политики и процедуры безопасности Информации.

Сотрудники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности Информации, а также о выявленных ими событиях, затрагивающих безопасность Информации, руководству подразделением и лицу, отвечающему за немедленное реагирование на угрозы безопасности Информации.

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

В соответствии со ст. 17 Федерального закона Российской Федерации от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» лица, виновные в нарушении требований данного Федерального закона, несут дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.

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 – пользователями ИСПДн правил, связанных с безопасностью Информации, они несут ответственность, установленную действующим законодательством Российской Федерации. Приведенные выше требования нормативных документов по защите информации должны быть отражены в должностных инструкциях сотрудников.

### Список использованных источников

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

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
3. Федеральный закон от 27 июля 2010 г. № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;
4. Постановление Правительства РФ от 24 октября 2011 г. № 861 «О федеральных государственных информационных системах, обеспечивающих предоставление в электронной форме государственных и муниципальных услуг (осуществление функций)»;
5. Постановление Правительства РФ от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
6. Постановление Правительства РФ от 21 марта 2012 г. № 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, выполняющими государственные функции и муниципальными органами исполнительной власти, органами государственных внебюджетных организаций, органами государственной власти субъектов Российской Федерации, органами местного самоуправления»;
7. Постановление Правительства РФ от 27 сентября 2011 г. № 797 «О взаимодействии между многофункциональными центрами предоставления государственных и муниципальных услуг и федеральными органами государственной власти субъектов Российской Федерации, содержащейся информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
8. Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Требования к защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;
9. Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Составы и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;
10. Приказ ФСБ РФ от 9 февраля 2005 г. № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)»;
11. Приказ ФАПСИ от 13 июня 2001 г. № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;
12. Методический документ «Меры защиты информации в государственных информационных системах» утвержденный ФСТЭК России 11 февраля 2014 г.;
13. «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную

- тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденные ФСБ России 21 февраля 2008 г. № 149/6/6-622.
14. «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденная заместителем директора ФСТЭК России 15 февраля 2008 г.;
15. «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утвержденная заместителем директора ФСТЭК России 15 февраля 2008 г.