УТВЕРЖДЕНО
Приказом заведующего МБДОУ
«Детский сад № 1 «Семицветик»
от «17» января 2017 № 17

ПОЛОЖЕНИЕ
по обеспечению безопасности данных при помощи средств криптографической защиты информации

г. Гаджиево, 2016г.

I. Общие положения

1.1. Настоящее Положение устанавливает требования к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, представляющих собой совокупность персональных данных, содержащихся в базах данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации (далее - информационные системы).

1.2. Под техническими средствами, позволяющими осуществлять обработку персональных данных, понимаются средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки персональных данных (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

1.3. 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.

1.4. Безопасность персональных данных при их обработке в информационных системах обеспечивается с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства (приложение 1), средства предотвращения несанкционированного доступа, утечки информации по техническим каналам, программно-технических воздействий на технические средства обработки персональных данных), а также используемые в информационной системе информационные технологии.

Технические и программные средства должны удовлетворять устанавливаемым в соответствии с законодательством Российской Федерации требованиям, обеспечивающим защиту информации.

1.5. Для обеспечения безопасности персональных данных при их обработке в информационных системах осуществляется защита речевой информации и информации, обрабатываемой техническими средствами, а также информации, представленной в виде информативных электрических сигналов, физических полей, носителей на бумажной, магнитной, магнитно-оптической и иной основе.

II. Методы и способы защиты информации в информационных системах

2.1. Методы и способы защиты информации в информационных системах устанавливаются Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий. Достаточность принятых мер по обеспечению безопасности персональных данных при их обработке в информационных системах оценивается при проведении государственного контроля и надзора.

2.2. Работы по обеспечению безопасности персональных данных при их обработке в информационных системах являются неотъемлемой частью работ по созданию информационных систем.

2.3. Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия.

2.4. Информационные системы классифицируются государственными органами, муниципальными органами, юридическими или физическими лицами, организующими и (или) осуществляющими обработку персональных данных, а также определяющими цели и содержание обработки персональных данных (далее - оператор), в зависимости от объема обрабатываемых ими персональных данных и угроз безопасности жизненно важным интересам личности, общества и государства.

Порядок проведения классификации информационных систем устанавливается совместно Федеральной службой по техническому и экспортному контролю, Федеральной службой безопасности Российской Федерации и Министерством информационных технологий и связи Российской Федерации.

2.5. Обмен персональными данными при их обработке в информационных системах осуществляется по каналам связи, защита которых обеспечивается путем реализации соответствующих организационных мер и (или) путем применения технических средств (н-р: программный продукт *ViPNet Client 3.2).*

2.6. Размещение информационных систем, специальное оборудование и охрана помещений, в которых ведется работа с персональными данными, организация режима обеспечения безопасности в этих помещениях должны обеспечивать сохранность носителей персональных данных и средств защиты информации (приложение 2), а также исключать возможность неконтролируемого проникновения или пребывания в этих помещениях посторонних лиц.

2.7. Возможные каналы утечки информации при обработке персональных данных в информационных системах определяются Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

III Безопасность персональных данных при их обработке в информационной системе

3.1. Безопасность персональных данных при их обработке в информационной системе обеспечивает оператор или лицо, которому на основании договора оператор поручает обработку персональных данных (далее - уполномоченное лицо). Существенным условием договора является обязанность уполномоченного лица обеспечить конфиденциальность персональных данных и безопасность персональных данных при их обработке в информационной системе.

3.2. При обработке персональных данных в информационной системе должно быть обеспечено:

а) проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

б) своевременное обнаружение фактов несанкционированного доступа к персональным данным;

в) недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;

г) возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;

д) постоянный контроль за обеспечением уровня защищенности персональных данных.

3.3. **Мероприятия** по обеспечению безопасности персональных данных при их обработке в информационных системах включают в себя:

а) определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;

б) разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;

в) проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;

г) установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;

д) обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

е) учет применяемых средств защиты информации, эксплуатационной и технической документации к ним, носителей персональных данных;
ж) учет лиц, допущенных к работе с персональными данными в информационной системе;
з) контроль за соблюдением условий использования средств защиты информации, предусмотренных эксплуатационной и технической документацией;
и) разбирательство и составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, которые могут привести к нарушению конфиденциальности персональных данных или другим нарушениям, приводящим к снижению уровня защищенности персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений;
к) описание системы защиты персональных данных.

IV. Ответственные за обеспечение безопасности персональных данных

4.1. Для разработки и осуществления мероприятий по обеспечению безопасности персональных данных при их обработке в информационной системе оператором или уполномоченным лицом может назначаться структурное подразделение или должностное лицо (работник), ответственные за обеспечение безопасности персональных данных (приложения 3,4).

4.2. Лица, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения служебных (трудовых) обязанностей, допускаются к соответствующим персональным данным на основании списка, утвержденного оператором или уполномоченным лицом.

4.3. Запросы пользователей информационной системы на получение персональных данных, включая лиц, указанных в пункте 4.2. настоящего Положения, а также факты предоставления персональных данных по этим запросам регистрируются автоматизированными средствами информационной системы в электронном журнале обращений. Содержание электронного журнала обращений периодически проверяется соответствующими должностными лицами (работниками) оператора или уполномоченного лица.

4.4. При обнаружении нарушений порядка предоставления персональных данных оператор или уполномоченное лицо незамедлительно приостанавливают предоставление персональных данных пользователям информационной системы до выявления причин нарушений и устранения этих причин.

V. Контроль и учет

5.1. Реализация требований по обеспечению безопасности информации в средствах защиты информации возлагается на их разработчиков.

5.2. В отношении разработанных шифровальных (криптографических) средств защиты информации, предназначенных для обеспечения безопасности персональных данных при их обработке в информационных системах, проводятся тематические исследования и контрольные тематические исследования в целях проверки выполнения требований по безопасности информации (приложения 5, 6). При этом под тематическими исследованиями понимаются криптографические, инженерно-криптографические и специальные исследования средств защиты информации и специальные работы с техническими средствами информационных систем, а под контрольными тематическими исследованиями - периодически проводимые тематические исследования.

Конкретные сроки проведения контрольных тематических исследований определяются Федеральной службой безопасности Российской Федерации.

5.3. Результаты оценки соответствия и (или) тематических исследований средств защиты информации, предназначенных для обеспечения безопасности персональных данных при их обработке в информационных системах, оцениваются в ходе экспертизы, осуществляемой Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

5.4. К средствам защиты информации, предназначенным для обеспечения безопасности персональных данных при их обработке в информационных системах, прилагаются правила пользования этими средствами, согласованные с Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

Изменение условий применения средств защиты информации, предусмотренных указанными правилами, согласовывается с этими федеральными органами исполнительной власти в пределах их полномочий.

5.5. Средства защиты информации, предназначенные для обеспечения безопасности персональных данных при их обработке в информационных системах, подлежат учету с использованием индексов или условных наименований и регистрационных номеров. Перечень индексов, условных наименований и регистрационных номеров определяется Федеральной службой по техническому и экспортному контролю и Федеральной службой безопасности Российской Федерации в пределах их полномочий.

5.6. Особенности разработки, производства, реализации и эксплуатации шифровальных (криптографических) средств защиты информации и предоставления услуг по шифрованию персональных данных при их обработке в информационных системах устанавливаются Федеральной службой безопасности Российской Федерации.

Приложение № 1
к Положению по обеспечению безопасности данных при помощи средств криптографической защиты информации

ЗАЯВЛЕНИЕ
на подключение к ЗСОО

Наименование учреждения _____
ИНН_____

**В случае подключения нескольких средств СКЗИ – указывать информацию обо всех*

СКЗИ №___

Адрес подключения	*Указывается фактический адрес установки СКЗИ (Город, почтовый адрес)….*
Наименование СКЗИ	*Указывается СКЗИ, с использованием, которого будет производиться подключение к ЗСОО (Пример: ViPNet Client 3.2; ViPNet Coordinator HW100A; ViPNet Coordinator HW100B; ViPNet Coordinator HW100C; ViPNet Coordinator HW1000)*
ФИО пользователя	*Заполняется только при подключении с использованием СКЗИ ViPNetClient*
Структурное подразделение	
Электронная почта	
Телефон	
Реквизиты приказа	

(*Все поля заполняются максимально полно. Фамилия, имя, отчество впечатываются в**ИМЕНИТЕЛЬНОМ ПАДЕЖЕ**, все поля заполняются исключительно в печатном виде, путем редактирования на компьютере с последующем распечатыванием на принтере. Заполнение «от руки» **НЕДОПУСТИМО**.)

Ответственным пользователем СКЗИ в _____
(наименование организации)
назначен _____
(ФИО)
(приказ от _____ № _____)

Поставщик СКЗИ _____
(наименование организации-поставщика СКЗИ)

Ответственный пользователь_____ /_____ /
Подпись
Руководитель учреждения _____ /_____/
Подпись

"____" _____ 201_ г
М.П.

Приложение № 2
к Положению по обеспечению безопасности
данных при помощи средств
криптографической защиты информации

Доверенность № _____
на получение средств криптографической защиты информации и электронно-цифровой подписи

Дата выдачи: _____
(дата прописью)

_____,
(наименование организации)

в лице _____,
(должность и ФИО руководителя - полностью)

действующего на основании _____

настоящей доверенностью уполномочивает _____

_____

(должность и ФИО – полностью)

(паспорт серии _____ № _____, выдан "___" _____

_____ года _____) представлять интересы
(кем выдан)

_____ и получить
(наименование организации)

средства криптографической защиты информации (СКЗИ), а так же дистрибутивы ключей для первичного запуска прикладной программы сети ViPNet и выполнить все необходимые действия, связанные с исполнением настоящего поручения.

Ответственным пользователем в _____
(наименование организации)

за эксплуатацию СКЗИ назначен _____
(Ф.И.О., занимаемая должность)

_____.

Доверенность действительна до "___" _____ 20___ года и дана без права передоверия.

Подпись лица, получившего доверенность _____.
(подпись)

Руководитель _____ (_____)

(подпись) *(инициалы и фамилия)*

М.П.

"____"_____20___г.

Приложение № 3
к Положению по обеспечению безопасности
данных при помощи средств
криптографической защиты информации

(наименование организации)

ПРИКАЗ

_____ № ___
(дата)

г. Гаджиево

О назначении ответственного пользователя средств криптографической защиты информации и лиц их замещающих

Для осуществления мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием средств криптографической защиты информации (далее – СКЗИ) информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, **п р и к а з ы в а ю:**

1. Назначить ответственным пользователем СКЗИ и возложить функции органа криптографической защиты по организации работ с СКЗИ, выработки соответствующих инструкций для пользователей, а также контролю за соблюдением требований по безопасности СКЗИ на следующего(-их) сотрудника(-ов):

_____
(Ф.И.О., должность, подразделение, e-mail, телефон)

_____
(Ф.И.О., должность, подразделение, e-mail, телефон)

2. Ответственному(-ым) пользователю(-ям) СКЗИ провести инструктаж и обучение пользователя(-ей) СКЗИ и ознакомить под роспись с правилами эксплуатации СКЗИ.

3. Ответственный пользователь обязан:

- контролировать соблюдения пользователями конфиденциальности при обращении со сведениями, которые им доверены или стали известны по работе, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых компонентов ЗСОО и ключевых документах к ним;
- проводить ознакомление пользователей с правилами работы и требованиями безопасности ЗСОО;
- осуществлять хранение эксплуатационной и технической документации, ключевых документов, носителей информации ограниченного распространения, относящихся к компонентам ЗСОО, в соответствии с требованиями законодательства;
- соблюдать правила эксплуатации СКЗИ;
- принимать меры по препятствованию несанкционированного доступа к

компонентам ЗСОО со стороны пользователей и иных посторонних лиц;

- немедленно принимать меры по предупреждению разглашения защищаемых персональных данных, а также возможной их утечки при выявлении фактов утраты или недостачи криптосредств, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.

4. Назначенные в соответствии с п. 1 настоящего приказа сотрудник(-и) несут персональную ответственность за:

- сохранение в тайне конфиденциальной информации, ставшей им известной в процессе обмена информацией;

- сохранение в тайне закрытых ключей шифрования и иной ключевой информации;

- соблюдение правил эксплуатации программно-аппаратных средств ViPNet.

5. Контроль за исполнением настоящего приказа оставляю за _____.

Руководитель учреждения _____ _____

Подпись Расшифровка

Приложение № 4
к Положению по обеспечению безопасности
данных при помощи средств
криптографической защиты информации

(наименование организации)

ПРИКАЗ

_____ № ___
(дата)

г. Гаджиево

О назначении пользователей
средств криптографической защиты информации

Для осуществления мероприятий по организации и обеспечению безопасности хранения, обработки и передачи с использованием СКЗИ информации с ограниченным доступом, не содержащей сведений составляющих государственную тайну, с использованием информационных систем ЗСОО **п р и к а з ы в а ю:**

1. Допустить к самостоятельной работе с СКЗИ следующих работников:

№	ФИО пользователя	Структурное подразделение	Должность

2. В своей работе пользователям СКЗИ руководствоваться нормативно-правовыми актами РФ в сфере защиты информации.

3. Контроль за исполнением настоящего приказа оставляю за _____.

Руководитель учреждения _____ _____
Подпись Расшифровка

Приложение № 5
к Положению по обеспечению безопасности
данных при помощи средств
криптографической защиты информации

Акт
о вводе СКЗИ в эксплуатацию

«___» _____ 20___ г.

Комиссия в составе: председателя комиссии _____ _____, членов комиссии _____ _____ и
Ответственного пользователя СКЗИ _____
составила акт о том, что (наименование СКЗИ) установлен в _____по адресу_____
в помещении №_____, в соответствии с технической и эксплуатационной документацией и введен в эксплуатацию.
Состав (наименование СКЗИ):
Системный блок № _____
Программный комплекс:
(наименование СКЗИ) версия _____ сборка _____
Версия операционной системы: _____
Дополнительно установленное ПО (антивирусное ПО, Прокси-сервер, ПО для удаленного администрирования и т. д.):
_____
_____
Дополнительно установленное оборудование (наименование, назначение, серийный номер и т. д.) _____

Председатель комиссии:

_____	_____	_____
Должность	Ф.И.О.	Подпись

Члены комиссии:

_____	_____	_____
Должность	Ф.И.О.	Подпись
_____	_____	_____
Должность	Ф.И.О.	Подпись

Приложение № 6
к Положению по обеспечению безопасности данных при помощи средств криптографической защиты информации

Протокол
контрольной проверки СКЗИ

«___» _____ 20___ г.

(наименование СКЗИ) установлен в _____ по адресу_____

в помещении №_____, в соответствии с технической и эксплуатационной документацией.

Состав (наименование СКЗИ):

Системный блок № _____

Программный комплекс:

(наименование СКЗИ) версия: _____

Версия операционной системы: _____

Дополнительно установленное оборудование (наименование, назначение, серийный номер и т.д) _____

Дополнительно установленное ПО (антивирусное ПО, Прокси-сервер, ПО для удаленного администрирования и т. д.): _____

Состав и результаты проверок и контрольных тестов

№	Описание действий	Ожидаемый результат	Результат (+/-)	Примечания. Отметки об устранении
1.	Загрузка ОС с отказом от ввода пароля ViPNet	Отказ в загрузке ОС		
2.	Загрузка ОС с аутентификацией пользователя[1]	Загрузка ОС и старт ПО ViPNet		
3.	Проверка установленных режимов безопасности[2]	Режимы безопасности соответствуют назначению СУ		
4.	Проверка настроек ПО	Настройки ПО соответствуют требованиям[3]		
5.	Аутентификация с паролем администратора СУ	Переход ПО в режим работы администратора СУ		
6.	Контроль журнала событий ПО ViPNet Координатор [Монитор]	Отсутствие попыток несанкционированного изменения режимов, настроек фильтров, аварийных завершений ПО		
7.	Контроль журнала регистрации IP-пакетов	Отсутствие признаков сетевых атак, отсутствие информации о пропуске		

[1] Указать тип аутентификации
[2] Для координаторов на каждом из сетевых интерфейсов
[3] Пункт 5.3.1, Регламент информационной безопасности при использовании программно-аппаратных средств комплекса ViPNet (ФРКЕ. 00029-04 90 01)

№	Описание действий	Ожидаемый результат	Результат (+/-)	Примечания. Отметки об устранении
		пакетов на запрещенные режимом (фильтрами) адреса (протоколы)		
8.	Проверка связи с видимыми СУ защищенной сети	Наличие сообщений о доступности СУ		
9.	Проверка связи с видимым СУ защищенной сети, для которого включен фильтр блокировки пакетов	Наличие сообщений о недоступности СУ, информация в журнале о блокировании пакетов		
10.	Проверка связи (ping _____) с открытым не зарегистрированным адресом (во 2 режиме)	Отсутствие ответа от узла. Информация в журнале о блокировке пакетов для данного адреса		
11.	Настройка фильтра, блокирующего отдельный протокол (например, ICMP) для отдельного СУ защищенной сети, проверка соединения с СУ по данному протоколу	Отсутствие ответа от СУ, информация о блокировании пакетов по выбранному протоколу		
12.	Настройка фильтра, запрещающего отдельный протокол (например, UDP) для всех СУ защищенной сети, проверка связи с СУ по данному протоколу (например, проверка соединения)	Наличие сообщений о недоступности СУ. Информация в журнале о блокировании пакетов		
13.	Настройка фильтра, разрешающего отдельный протокол (например, ICMP) для всех узлов открытой сети, проверка связи с любым открытым узлом по данному протоколу (например, ping)	Наличие ответа от узла. Информация в журнале о пропуске пакетов для данного адреса		
14.	Проверка связи по разрешенному протоколу для зарегистрированных открытых адресов[4]	Наличие соединения по данному протоколу		
15.	Проверка связи по запрещенному протоколу для зарегистрированных открытых адресов	Отсутствие соединения по данному протоколу		
16.	Отправка зашифрованного и подписанного письма адресатам ДП[5]	Отправка письма, получение квитанций о доставке (прочтении)		
17.	Контроль журналов автопроцессинга ДП[6]	Отсутствие сбоев в работе правил		

ОТВЕТСТВЕННЫЙ ПОЛЬЗОВАТЕЛЬ СКЗИ

ФИО _____

Дата: «___» _____ 20___ г.
Подпись: _____
М.П.

[4] Только для 2 режима безопасности
[5] При наличии установленного ПО ViPNet Клиент [Деловая Почта]
[6] При наличии данного функционала на СУ