КОМИТЕТ
РЕСПУБЛИКИ СЕВЕРНАЯ ОСЕТИЯ-АЛАНИЯ
ПО ЗАНЯТОСТИ НАСЕЛЕНИЯ

ПРИКАЗ

«27» 11 2024 г. № 64-р

г. Владикавказ

Об утверждении организационных и технических мер по обеспечению безопасности персональных данных ПДн при их обработке в ИСПДн с использованием СКЗИ Комитета РСО-Алания по занятости населения

В соответствии с приказом Федеральной службы безопасности Российской Федерации от 10 июля 2014 года №378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требования к защите персональных данных для каждого из уровней защищенности», приказом Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 года №21 « Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» **приказываю**:

1. Утвердить состав и содержание организационных и технических мер по обеспечению безопасности персональных данных ПДн при их обработке в информационных системах персональных данных ИСПДн Комитета РСО-Алания по занятости населения.
2. Козаевой И.Б. - ведущему советнику отдела организационной, кадровой работы и противодействия коррупции ознакомить с приказом касающихся лиц под роспись.
3. Контроль исполнения приказа возложить на начальника отдела информационных технологий и автоматизации Чельдиеву М.К.

Заместитель председателя **Э.Л. Авакова**

Администрация Главы РСО-Алания
Правительства РСО-Алания
ЗАРЕГИСТРИРОВАНО
28 11 2024
№ 0338-24-2

Утверждены
приказом Комитета РСО-Алания
по занятости населения
от 21.11.2024 года № 69-ф

СОСТАВ И СОДЕРЖАНИЕ ОРГАНИЗАЦИОННЫХ И ТЕХНИЧЕСКИХ МЕР ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ КОМИТЕТА РСО-АЛАНИЯ ПО ЗАНЯТОСТИ НАСЕЛЕНИЯ

г.Владикавказ
2024 г.

1.Общие положения

Настоящий документ устанавливает состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (далее - ИСПДн).

Меры по обеспечению безопасности персональных данных принимаются для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных (далее - ПДн).

Меры по обеспечению безопасности персональных данных при их обработке в государственных информационных системах принимаются в соответствии с требованиями о защите информации, содержащейся в государственных информационных системах, устанавливаемыми ФСТЭК России в пределах своих полномочий в соответствии с частью 5 статьи 16 Федерального закона от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации».

В состав применяемых средств зашиты, категорий персональных данных, категории вероятных нарушителей входят следующие угрозы безопасности для ИСПДн Комитета Республики Северная Осетия-Алания (далее- Комитет):

-угрозы утечки акустической информации;
-угрозы утечки видовой информации;
-угрозы, реализуемые в ходе загрузки операционной системы;
-угрозы, реализуемые после загрузки операционной системы;
-угрозы внедрения вредоносных программ;
-угрозы «Анализ сетевого трафика» с перехватом передаваемой по сети информации;
-угрозы выявления паролей;
-угрозы удаленного запуска приложений;
-угрозы внедрения по сети вредоносных программ.
-угрозы сканирования, направленные на выявление открытых портов и служб, открытых соединений и др.

Безопасность ПДн при их обработке в информационных системах должна обеспечиваться с помощью системы защиты персональных данных, включающей организационные меры и средства защиты информации (в том числе шифровальные (криптографические) средства, 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.

2. Состав и содержание мер по обеспечению безопасности персональных данных ПДн

В состав мер по обеспечению безопасности ПДн, реализуемых в рамках системы защиты персональных данных с учетом актуальных угроз безопасности входит:

2.1. Идентификация и аутентификация субъектов доступа и объектов доступа.

Возникновение угроз утечки акустической (речевой) информации, содержащей непосредственно в произносимой речи пользователя при обработке ПДн в ИСПДн, обусловлено наличием функции голосового ввода ПДн в ИСПДн или функций воспроизведения ПДн акустическими средствами ИСПДн. В ИСПДн функции голосового ввода информации или функции воспроизведения ПДн акустическими средствами отсутствуют. Данные угрозы в используемых ИСПДн Комитета отсутствуют.

2.2 Управление доступом субъектов доступа к объектам доступа.

Управление доступами к ИСПДн осуществляется посредством предоставления пользователям прав доступа к объектам доступа информационной системы, основываясь на задачах, решаемых пользователями в информационной системе и взаимодействующими с ней информационными системами. Типы доступа включают операции по чтению, записи, удалению, выполнению иных операций, разрешенные к выполнению пользователем (группе пользователей) или запускаемому от его имени процессу при доступе к объектам доступа. Правила разграничения доступа реализуются на основе установленных администратором ИСПДн списков доступа и должны обеспечивать управление доступом пользователей (групп пользователей) и запускаемых от их имени процессов при входе в систему, доступе к техническим средствам, устройствам, объектам файловой системы, запускаемым и исполняемым модулям, объектам систем управления базами данных, объектам, создаваемым прикладным и специальным программным обеспечением, параметрам настройки средств защиты информации, информации о конфигурации системы защиты информации и иной информации о функционировании системы защиты информации, а также иным объектам доступа.

2.3 Защита машинных носителей информации, на которых хранятся и (или) обрабатываются персональные данные.

Защита машинных носителей на которых хранится информация с ПДн (средств обработки (хранения) персональных данных, съемных машинных носителей персональных данных) предотвращает возможность несанкционированного доступа к машинным носителям и хранящимся на них персональным данным, а также несанкционированное использование съемных машинных носителей ПДн.

2.4 Антивирусная защита.

Антивирусная защита ИСПДн обеспечивает обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ.

2.5 Контроль и мониторинг защищенности ПДн.

При работе с ПДн обеспечивается контроль уровня защищенности персональных данных, обрабатываемых в информационной системе, путем проведения систематических мероприятий по анализу защищенности информационной системы и тестированию работоспособности системы защиты ПДн.

2.6 Обеспечение целостности информационной системы и персональных данных.

Для выполнения меры проводится мониторинг работ по обнаружению фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней ПДн, а также возможность восстановления информационной системы и содержащихся в ней ПДн.

2.7 Защита технических средств.

Меры по защите технических средств направлены на исключение несанкционированного доступ к стационарным техническим средствам, обрабатывающим персональные данные, средствам, обеспечивающим функционирование информационной системы (далее - средства обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту персональных данных, представленных в виде информативных электрических сигналов и физических полей.

2.8 Защита информационной системы, ее средств, систем связи и передачи данных.

Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту персональных данных при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы и проектных решений, направленных на обеспечение безопасности персональных данных -выявление инцидентов (одного события или группы событий), которые

могут привести к сбоям или нарушению функционирования информационной системы и к возникновению угроз безопасности персональных данных, и реагирование на них.

2.9 Управление конфигурацией информационной системы и системы защиты персональных данных.

Меры по управлению конфигурацией информационной системы и системы защиты персональных данных обеспечиваются управлением конфигурации информационной системы и системы защиты персональных данных, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений.

В соответствии с приказом ФСБ Росси от 10 июля 2014 г. №378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных правительством российской федерации требований к защите персональных данных для каждого из уровней защищенности» утверждены следующие меры по обеспечению безопасности ПДн с использованием средств криптографической защиты информации (далее - СКЗИ):

-организован режим обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

- обеспечение сохранности носителей персональных данных;

-приказом Комитета утвержден перечень лиц, доступ которых к ПДн, обрабатываемым в информационной системе, необходим для выполнения ими служебных обязанностей;

- использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации;

- выполняется режим, препятствующий возможности неконтролируемого проникновения или пребывания в помещениях посторонних лиц, где размещены используемые СКЗИ;

- утверждены правила доступа в Помещения в рабочее и нерабочее время, а также в нештатных ситуациях;

в) утверждены списки сотрудников, имеющих право доступа в Помещения, где установлены СКЗИ.

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

При выявлении технических мер по обеспечению безопасности ПДн с учетом не выбранных ранее мер, приведенных в приложении к настоящему документу, в результате чего определяются меры по обеспечению безопасности ПДн, направленные на нейтрализацию всех актуальных угроз безопасности персональных данных для конкретной информационной системы.

3. Объекты защиты ИСПДн

К объектам защиты ИСПДн относятся:

3.1 Информация ПДн, хранящаяся или обрабатывающаяся на серверах, автоматизированных рабочих мест АРМ, других ИСПДн (Федеральные информационные ресурсы).

3.2 Конфигурационная и управляющая информация.

3.3 Информация в электронных журналах регистрации.

3.4 Резервные копии файлов с защищаемой информацией.

3.5 Остаточная информация на носителях информации.

3.6 Система защиты информации, в том числе ключевая и аутентифицирующая

пользователей информации.
3.7 Общесистемное и прикладное программное обеспечение серверов, АРМ.
3.8 Аппаратные средства узлов: оборудование серверов, АРМ, коммуникативного оборудования.
3.9 Кабельные коммуникации.
3.10 Системы СКЗИ.

4. Мероприятия по защите от угроз безопасности ПДн с использованием СКЗИ

Основные меры по защите ИСПДн с использованием СКЗИ отражены в таблице 1:

Таблица 1

№ п/п	Угрозы безопасности ПДн	Организационно-технические меры	Использование СКЗИ
1	**Угрозы утечки информации по техническим каналам**		
1.1	Угрозы утечки видовой информации		
1.1.1	Визуальный просмотр на экранах дисплеев и других средств отображения СВТ, ИВК, входящих в состав ИСПДн.	Контроль доступа в помещение ИСПДн. Размещение монитора, препятствующее просмотру экрана посторонним лицам.	
2	**Угрозы несанкционированного доступа НСД в ИСПДн**		
2.1	Угрозы возникновения непреднамеренных уязвимостей или сбоев в ИСПДн:		
2.1.1	Неверные настройки программного обеспечения ПО, изменение режимов работы технических средств ТС и ПО (случайное либо преднамеренное).	Проверка системы перед вводом в эксплуатацию, и при обновлениях.	
2.2	Угрозы непосредственного доступа в операционную среду ИСПДн:		
2.2.1	Доступ к информации и командам, хранящимся в BIOS с возможностью перехвата управления загрузкой операционной системы ОС и получения прав доверенного пользователя	Контроль доступа в помещение ИСПДн. Выполнение требований эксплуатационной документации.	СКЗИ НСД
2.2.2	Доступ в операционную среду (локальную ОС отдельного ТС ИСПДн) с возможностью выполнения НСД вызовом штатных процедур или запуска специально разработанных программ.	Контроль доступа в помещение ИСПДн. Выполнение требований эксплуатационной документации.	СКЗИ НСД
2.2.3	Доступ в среду функционирования прикладных программ (локальная ИСПДн).	Контроль доступа в помещение ИСПДн. Выполнение требований эксплуатационной документации.	СКЗИ НСД
2.2.4	Доступ непосредственно к информации пользователя, обусловленных возможностью нарушения ее конфиденциальности, целостности, доступности.	Контроль доступа в помещение ИСПДн Выполнение требований эксплуатационной документации.	СКЗИ НСД
2.3	Угрозы, реализуемые с использованием протоколов межсетевого взаимодействия:		
2.3.1	Сканирование сети и анализ сетевого трафика для изучения работы ИСПДн, выявления протоколов, портов, перехвата	Обучение и обеспечение лояльности пользователей и администраторов.	Средства межсетевого экранирования «ViPNet Custom»

	служебных данных (в том числе, идентификаторов и паролей), их подмены.	Выполнение требований эксплуатационной документации.	
2.3.2	Применение специальных программ для выявления паролей для ИСПДн.	Выполнение требований эксплуатационной документации.	Средства межсетевого экранирования «ViPNet Custom»
2.3.3	Подмена доверенного объекта сети с присвоением его прав доступа, внедрение ложного объекта сети.	Выполнение требований эксплуатационной документации.	Средства межсетевого экранирования «ViPNet Custom»
2.3.4	Реализация угрозы отказа в обслуживании.	Своевременное обновление ПО Выполнение требований эксплуатационной документации.	Средства межсетевого экранирования «ViPNet Custom»
2.3.5	Внедрение специализированных троянов, вредоносных программ.	Своевременное обновление ПО. Регламентация порядка защиты от вредоносных программ	Средства межсетевого экранирования «ViPNet Custom». Средства антивирусной защиты
2.3.6	Сетевые атаки	Своевременное обновление ПО. Контроль установленного ПО. Выполнение требований эксплуатационной документации.	Средства межсетевого экранирования «ViPNet Custom»
2.3.7	Применение утилит скрытого администрирования сети.	Обучение и обеспечение лояльности пользователей и администраторов	Средства межсетевого экранирования «ViPNet Custom». СКЗИ НСД
2.4	Угрозы несанкционированного физического доступа к техническим средствам ТС и системам обеспечения:		
2.4.1	Хищение сервера.	Соблюдение регламентированного порядка доступа в помещения с использованием ИСПДн. Применение системы контроля и управления доступом.	-
2.4.2	Нарушение функционирования сервера, рабочих станций.	Контроль доступа к узлу. Обучение и обеспечение лояльности пользователей и администраторов. Резервное копирование информации.	-
2.4.3	Доступ к системам обеспечения, их повреждение.	Соблюдение регламентированного порядка доступа в помещения с использованием ИСПДн.	-

		Применение системы контроля и управления доступом.	
2.4.4	Доступ к снятым с эксплуатации носителям информации (содержащим остаточные данные).	Учет носителей информации. Контроль использования носителей информации. Гарантированное физическое уничтожение носителей информации.	Средства гарантированного уничтожения информации, согласно регламента.
2.4.5	Хищение компьютерной техники	Соблюдение регламентированного порядка доступа в помещения с использованием ИСПДн. Применение системы контроля и управления доступом.	-
2.5	Угрозы неправомерных действий со стороны лиц, имеющих право доступа к информации:		
2.5.1	Разглашение информации лицам, не имеющим права доступа к ней.	Закрепление ответственности за разглашение информации по ПДн.	-
2.5.2	Несанкционированное изменение информации.	Регламентация порядка работы с ИСПДн. Резервирование информации. Контроль целостности информации.	СКЗИ НСД
2.5.3	Несанкционированное копирование информации (в том числе печать).	Контроль использования носителей информации. Выполнение требований эксплуатационной документации.	СЗИ НСД
2.5.4	Копирование информации на незарегистрированный носитель информации, в том числе распечатка ПДн.	Запрет использования посторонних носителей информации. Учет носителей информации. Контроль использования носителей информации. Маркировка распечаток.	СЗИ НСД
2.5.5	Передача носителя информации лицу, не имеющему права доступа к имеющейся на нем информации.	Закрепление ответственности за разглашение. Учет носителей информации. Контроль использования носителей информации. Средства опечатывания корпуса компьютерной техники.	СЗИ НСД

5. Заключение

Нарушение мер по защите от угроз безопасности ИСПДн может приводить к нарушению функционирования системы защиты ПДн Комитета. Нарушение целостности информации в электронных журналах регистрации может скрыть попытки реализации НСД к ПДн.

Использование криптографически опасной информации создает предпосылки для нарушения конфиденциальности ПДн.