УТВЕРЖДЕНА
приказом директора областного
государственного бюджетного
учреждения «Комплексный центр
социального обслуживания
Еврейской автономной области»

от 12.04.2021 г. № 122

ПОЛИТИКА
ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
информационных систем персональных данных
областного государственного бюджетного учреждения
«Комплексный центр социального обслуживания
Еврейской автономной области»

г. Биробиджан
2021 год

СОДЕРЖАНИЕ

	Определения	2
	Обозначения и сокращения ……..	7
	Введение ….....	8
1	Общие положения….....	10
2	Область действия ….....	10
3	Система защиты персональных данных….....	10
4	Объекты защиты……..	11
5	Пользователи ИСПДн ….....	12
5.1	Администратор информационной безопасности ….....	12
5.2	Пользователь ИСПДн/оператор АРМ ….....	12
5.3	Специалист по технической поддержке (технический специалист по обслуживанию периферийного оборудования)…..……	13
6	Должностные обязанности пользователей ИСПДн….....	13
7	Основные принципы построения системы защиты информации…..	14
8	Определение уровня защищённости ПДн……	17
9	Требования к подсистемам СЗПДн……...	18
10	Меры, методы и средства обеспечения требуемого уровня защищённости…….....	20
11	Требования к персоналу по обеспечению защиты ПДн……..	24
12	Ответственность работников Учреждения……..…	25
13	Контроль эффективности СЗПДн……..	25
14	Ожидаемый эффект от реализации Политики……..	26
	Приложение 1 «Уровни защищённости ПДн»…….	27
	Приложение 2 «Содержание мер по обеспечению безопасности персональных данных»……...	28
	Приложение 3 «Регистрация изменения локального нормативного документа»……...	34

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 отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность персональных данных – состояние защищённости персональных данных, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность персональных данных при их обработке в информационных системах персональных данных.

Биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

Блокирование персональных данных – временное прекращение сбора, систематизации, накопления, использования, распространения, персональных данных, в том числе их передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами не-санкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Вспомогательные технические средства и системы – технические средства и системы, не предназначенные для передачи, обработки и хранения персональных данных, устанавливаемые совместно с техническими средствами и системами, предназначенными для обработки персональных данных или в помещениях, в которых установлены информационные системы персональных данных.

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

Доступ к информации – возможность получения информации и её использования.

Закладочное устройство – элемент средства съёма информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съёма информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные

средства, а также в технические средства и системы обработки информации).

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

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация (персональные данные) обрабатываемая в информационной системе персональных данных.

Информационная система персональных данных (ИСПДн) – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

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

Использование персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта персональных данных или других лиц либо иным образом затрагивающих права и свободы субъекта персональных данных или других лиц.

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

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

Конфиденциальность персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределённое программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в информационную систему персональных данных и (или) выходящей из информационной системы.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности персональных данных при их обработке техническими средствами в

информационных системах персональных данных.

Неавтоматизированная обработка персональных данных – обработка персональных данных, содержащихся в информационной системе персональных данных либо извлечённых из такой системы, считается осуществлённой без использования средств автоматизации (неавтоматизированной), если такие действия с персональными данными, как использование, уточнение, распространение, уничтожение персональных данных в отношении каждого из субъектов персональных данных, осуществляются при непосредственном участии человека.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, 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 персональных данных.

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.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Обработка персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение персональных данных.

Общедоступные персональные данные – персональные данные, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта персональных данных или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности.

Оператор (персональных данных) – государственный орган, муниципальный орган, юридическое или физическое лицо, организующее и (или) осуществляющее обработку персональных данных, а также определяющие цели и содержание обработки персональных данных.

Технические средства информационной системы персональных данных – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приёма и обработки ПДн (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.

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

Персональные данные – любая информация, относящаяся к определённому или определяемому на основании такой информации 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.

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

Пользователь информационной системы персональных данных – лицо, участвующее в функционировании информационной системы персональных данных или использующее результаты её функционирования.

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

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

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

Раскрытие персональных данных – умышленное или случайное нарушение конфиденциальности персональных данных.

Распространение персональных данных – действия, направленные на передачу персональных данных определённому кругу лиц (передача персональных данных) или на ознакомление с персональными данными неограниченного круга лиц, в том числе обнародование персональных данных в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к персональным данным каким-либо иным способом.

Резервная копия – копия рабочей информации, полученная в результате резервного копирования.

Резервное копирование – процесс создания копий рабочей информации на определённый момент времени, направленный на предотвращение нарушения целостности и/или доступности рабочей информации и на её восстановление после таких нарушений.

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

Сети общего пользования – любые сети передачи данных (например, Интернет), в которых передаваемая информация может стать известна третьим лицам.

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

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

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

Трансграничная передача персональных данных – передача персональных данных оператором через Государственную границу Российской Федерации органу власти иностранного государства, физическому или юридическому лицу иностранного государства.

Угрозы безопасности персональных данных – совокупность условий и факторов, создающих опасность 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 при их обработке в информационной системе персональных данных.

Уничтожение персональных данных – действия, в результате которых невозможно восстановить содержание персональных данных в информационной системе персональных данных или в результате которых уничтожаются материальные носители персональных данных.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

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

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

Электронный носитель – носитель (например, компакт-диск, съёмный жёсткий диск и иной носитель информации), который может быть подключен к выделенным серверам и/или автоматизированным рабочим местам Учреждения и может быть использован для обработки, хранения и копирования на него информации.

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АИБ – администратор информационной безопасности
АС – автоматизированная система
АРМ – автоматизированное рабочее место
ИБ – информационная безопасность
ИСПДн – информационная система персональных данных
КЗ – контролируемая зона
НПА РФ – нормативные правовые акты Российской Федерации
НСД – несанкционированный доступ
ОС – операционная система
ПДн – персональные данные
ПО – программное обеспечение
СЗИ – средства защиты информации
СЗПДн – система защиты персональных данных
СОВ – система обнаружения вторжений
СОП – сеть общего пользования
УБПДн – угрозы безопасности персональных данных

ВВЕДЕНИЕ

Обеспечение информационной безопасности – необходимое условие для успешного осуществления уставной деятельности Учреждения.

Настоящая Политика информационной безопасности (далее – Политика, Политика ИБ) информационных систем персональных данных ОГБУ «Комплексный центр социального обслуживания Еврейской автономной области» (далее – Учреждение) является основополагающим документом, предназначенным для выражения позиции Учреждения в области информационной безопасности.

Под информационной безопасностью ПДн понимается защищённость ПДн и обрабатывающей их инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, её владельцам (субъектам ПДн) или инфраструктуре.

Политика ИБ – набор механизмов, посредством которых будут определены и достигнуты:

- конфиденциальность информации – обеспечение информацией только тех людей, которые уполномочены на получение такого доступа; хранение и просмотр конфиденциальной информации только теми людьми, кто по своим служебным обязанностям и полномочиям имеет на это право;

- целостность информации – защита конфиденциальной информации от неправомочной модификации; реализация Политики ИБ гарантирует, что информация не повреждена, не разрушена или не изменена любым способом.

- доступность информации – обеспечение возможности за приемлемое время получить требуемую информационную услугу, реализация Политики ИБ гарантирует, что информация всегда доступна и поддерживается в пригодном состоянии.

Политика является методологической основой для:

- принятия управленческих решений и разработки практических мер для реализации политики безопасности ПДн и выработки комплекса согласованных мер нормативно-правового, технологического и организационно-технического характера, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз ПДн;

- координации деятельности структурных подразделений Учреждения при проведении работ по развитию и эксплуатации ИСПДн с соблюдением требований обеспечения безопасности ПДн;

- разработки предложений по совершенствованию правового, нормативного, методического, технического и организационного обеспечения безопасности ПДн в ИСПДн Учреждения.

Политика разработана в соответствии с требованиями Федерального Закона от 27 июля 2006 № 152-ФЗ «О персональных данных», Постановления Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и Приказа ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», на основании:

- «Рекомендаций по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных», утверждённых Заместителем директора ФСТЭК России от 15.02.2008 г.

В Политике ИБ определены требования к работникам Учреждения, задействованным в работе с ИСПДн, степень ответственности персонала, структура и необходимый уровень защищённости, статус и должностные обязанности сотрудников, ответственных за обеспечение безопасности персональных данных в архивах и ИСПДн Учреждения.

Настоящая Политика является локальным нормативным документом постоянного действия.

Принятием настоящей Политики Оператор обязуется осуществлять все возможные меры для защиты работников, получателей социальных услуг, имущества, информации, деловой репутации Учреждения от риска причинения вреда, убытков и ущерба, возникающих в результате реализации угроз информационной безопасности.

1. ОБЩИЕ ПОЛОЖЕНИЯ

Целью настоящей Политики является обеспечение эффективного противодействия внутренним и внешним, умышленным и непреднамеренным угрозам, направленным на нарушение процессов сбора, обработки, хранения и предоставления информации, минимизация ущерба от возможной реализации угроз безопасности ПДн.

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

Информация и связанные с ней ресурсы должны быть доступны только для авторизованных пользователей. Должно осуществляться своевременное обнаружение и реагирование на УБПДн и предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

2. ОБЛАСТЬ ДЕЙСТВИЯ

Требования настоящей Политики распространяются на всех работников Учреждения (штатных, временных, работающих по контракту и т.п.), а также всех прочих лиц (получатели социальных услуг, подрядчики, аудиторы и т.п.).

3. СИСТЕМА ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Система защиты персональных данных (СЗПДн) представляет собой совокупность организационных и технических мероприятий для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения ПДн, а также иных неправомерных действий с ними.

Для достижения основной цели система защиты персональных данных должна эффективно обеспечивать:

- защиту от вмешательства в процесс функционирования ИСПДн посторонних лиц (возможность использования ИСПДн и доступ к её ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);

- разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам ИСПДн (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям ИСПДн для выполнения своих должностных обязанностей);

- контроль целостности (обеспечение неизменности) среды исполнения программ и её восстановление в случае нарушения;

- защиту от несанкционированной модификации и контроль целостности используемых в ИСПДн программных средств, а также защиту системы от внедрения несанкционированных программ;

- защиту ПДн от утечки по техническим каналам при их обработке, хранении и передаче по каналам связи;

- защиту ПДн, хранимых, обрабатываемых и передаваемых по каналам связи, от несанкционированного разглашения или искажения;

- своевременное выявление источников угроз безопасности ПДн, причин и условий, способствующих нанесению ущерба субъектам ПДн, создание механизма оперативного реагирования на угрозы безопасности ПДн и негативные тенденции;

- создание условий для минимизации и локализации наносимого неправомерными действиями физических и юридических лиц ущерба, ослабления негативного влияния и ликвидация последствий нарушения безопасности ПДн.

Система защиты персональных данных строится на основании:

- Отчёта о результатах проведения внутренней проверки;
- Перечня персональных данных, подлежащих защите;
- частной Модели угроз безопасности персональных данных;
- Положения о разграничении прав доступа к обрабатываемым персональным данным (Матрица доступа);
- руководящих документов ФСТЭК и ФСБ России.

На основании этих документов и анализа актуальных угроз безопасности ПДн, описанного в Модели угроз и Отчёте о результатах проведения внутренней проверки, определяется необходимый уровень защищённости ПДн каждой ИСПДн Учреждения и делается заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности ПДн.

4. ОБЪЕКТЫ ЗАЩИТЫ

Объекты защиты включают в себя:

1) обрабатываемую информацию;
2) технологическую информацию;
3) программно-технические средства обработки;
4) каналы информационного обмена;
5) помещения, в которых размещены компоненты ИСПДн.

5. ПОЛЬЗОВАТЕЛИ ИСПДн

Пользователем ИСПДн является специалист Учреждения, имеющий доступ к ресурсам ИСПДн в соответствии с установленным порядком и его функциональными обязанностями.

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

- администратор информационной безопасности ИСПДн;
- пользователь ИСПДн (оператор АРМ);
- специалист по технической поддержке (технический специалист по обслуживанию периферийного оборудования).

5.1. Администратор информационной безопасности ИСПДн

Администратор информационной безопасности – сотрудник Учреждения, ответственный за функционирование СЗПДн, включая обслуживание и настройку. Администратор безопасности ИСПДн обладает следующим уровнем доступа и знаний:

- обладает правами Администратора ИСПДн (системного администратора);
- 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 Политику безопасности в части настройки системы контроля защиты информации (СКЗИ), в соответствии с которыми пользователь (оператор АРМ) получает возможность работать с элементами ИСПДн;
- осуществлять аудит средств защиты;
- устанавливать доверительные отношения своей защищённой сети с сетями других подразделений.

5.2. Пользователь ИСПДн/оператор АРМ

Пользователь/оператор АРМ – специалисты подразделений Учреждения, осуществляющие обработку ПДн. Обработка ПДн включает: возможность просмотра ПДн, ручной ввод ПДн в систему ИСПДн, формирование справок и отчётов по информации, полученной из ИСПДн. Оператор не имеет полномочий для управления подсистемами обработки данных и СЗПДн.

Оператор АРМ 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.

5.3. Специалист по технической поддержке (Технический специалист по обслуживанию периферийного оборудования)

Специалист по технической поддержке – сотрудник Учреждения, осуществляющий обслуживание и настройку периферийного оборудования ИСПДн.

Технический специалист по обслуживанию обладает следующим уровнем доступа и знаний:

- обладает правами внесения изменений в программное обеспечение ИСПДн на стадии её разработки, внедрения и сопровождения;
- обладает информацией о системном и прикладном программном обеспечении ИСПДн;
- располагает всей информаций о технических средствах обработки и защиты ПДн, обрабатываемых в ИСПДн;
- обладает правами конфигурирования и административной настройки технических средств ИСПДн.

6. ДОЛЖНОСТНЫЕ ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ ИСПДн

Должностные обязанности пользователей ИСПДн описаны в следующих локальных актах:

- Инструкция администратора информационной безопасности ИСПДн ОГБУ «КЦСО ЕАО»;
- Инструкция пользователя информационных систем персональных данных ОГБУ «КЦСО ЕАО» в части обеспечения безопасности ПДн при их обработке в ИСПДн;
- Инструкция пользователя информационных систем персональных данных по обеспечению безопасности обработки персональных данных при возникновении нештатных ситуаций;
- Инструкция специалиста по технической поддержке;
- Инструкция пользователя ИСПДн по организации работ на случай возникновения нештатных ситуаций.

Категории пользователей определяются для каждой ИСПДн, уточняется разделение специалистов внутри категорий в соответствии с типами пользователей, определёнными в Политике информационной безопасности информационных систем персональных данных ОГБУ «КЦСО ЕАО».

Данные о группах пользователей, уровне их доступа и информированности должны быть отражены в Матрице доступа к обрабатываемым персональным данным в информационных системах персональных данных Учреждения.

7. ОСНОВНЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Построение системы обеспечения безопасности ПДн ИСПДн ОГБУ «КЦСО ЕАО» и её функционирование осуществляются в соответствии со следующими основными принципами:

1) законность;
2) системность;
3) комплексность;
4) непрерывность;
5) своевременность;
6) преемственность и непрерывность совершенствования;
7) персональная ответственность;
8) минимизация полномочий;
9) взаимодействие и сотрудничество;
10) гибкость системы защиты;
11) открытость алгоритмов и механизмов защиты;
12) простота применения средств защиты;
13) научная обоснованность и техническая реализуемость;
14) специализация и профессионализм;
15) обязательность контроля.

7.1. Законность

Предполагает осуществление защитных мероприятий и разработку СЗПДн Учреждения в соответствии с требованиями законодательства в области защиты ПДн и других нормативных актов по безопасности информации, утверждённых органами государственной власти в пределах их компетенции.

Пользователи и обслуживающий персонал ИСПДн Учреждения должны быть осведомлены о порядке работы с защищаемой информацией и об ответственности за защиту ПДн.

7.2. Системность

При создании СЗПДн должны учитываться все слабые и наиболее уязвимые места системы обработки ПДн, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределённые системы и НСД к информации. СЗПДн должна строиться с учётом не только всех известных каналов проникновения и НСД к информации, но и с учётом возможности появления принципиально новых путей реализации угроз безопасности.

7.3. Комплексность

Комплексное использование методов и средств защиты ПДн предполагает согласованное применение разнородных средств при построении целостной СЗПДн, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных её компонентов.

Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей.

Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

7.4. Непрерывность

Защита ПДн – не разовое мероприятие и не простая совокупность проведённых мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИСПДн.

ИСПДн должны находиться в защищённом состоянии на протяжении всего времени их функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода ИСПДн в незащищённое состояние.

Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная техническая и организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имён, паролей, ключей шифрования, переопределение полномочий и т.п.).

7.5. Своевременность

Предполагает упреждающий характер мер обеспечения безопасности ПДн, то есть постановку задач по комплексной защите ИСПДн и реализацию мер обеспечения безопасности ПДн на ранних стадиях разработки ИСПДн в целом и её системы защиты информации, в частности.

7.6. Преемственность и непрерывность совершенствования

Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования ИСПДн и её системы защиты с учётом нормативных требований по защите.

7.7. Персональная ответственность

Предполагает возложение ответственности за обеспечение безопасности ПДн и системы их обработки на каждого специалиста в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей специалистов строится таким образом, чтобы в случае любого нарушения круг виновников был чётко известен или сведён к минимуму.

7.8. Минимизация полномочий

Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью, на основе принципа «все, что не разрешено, запрещено». Доступ к ПДн должен предоставляться только в том случае и в том объёме, который необходим специалисту для выполнения его должностных обязанностей.

7.9. Взаимодействие и сотрудничество

Предполагает создание благоприятной атмосферы в коллективах подразделений, обеспечивающих деятельность ИСПДн Учреждения, для снижения вероятности возникновения негативных действий, связанных с человеческим фактором. В такой обстановке специалисты должны осознанно соблюдать установленные правила и оказывать содействие в деятельности ответственного за функционирование ИСПДн.

7.10. Гибкость системы защиты

Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищённости средства защиты должны обладать определённой гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса её нормального функционирования.

7.11. Открытость алгоритмов и механизмов защиты

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счёт секретности структурной организации и алгоритмов функционирования её подсистем. Знание алгоритмов работы системы защиты не должно давать возможности её преодоления (даже авторам). Однако это не означает, что информация о конкретной системе защиты должна быть общедоступна.

7.12. Простота применения средств защиты

Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе

зарегистрированных в установленном порядке пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имён и т.д.).

Должна достигаться автоматизация максимального числа действий пользователей и администраторов ИСПДн.

7.13. Научная обоснованность и техническая реализуемость

Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации и должны соответствовать установленным нормам и требованиям по безопасности ПДн.

СЗПДн должна быть ориентирована на решения, возможные риски для которых и меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

7.14. Специализация и профессионализм

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности ПДн, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами КЦСОН.

7.15. Обязательность контроля

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности ПДн на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации, должен охватывать как несанкционированные, так и санкционированные действия пользователей.

8. ОПРЕДЕЛЕНИЕ УРОВНЯ ЗАЩИЩЁННОСТИ ПДН

При обработке персональных данных в ИСПДн Учреждения устанавливаются уровни защищённости ПДн в соответствии с Постановлением Правительства от 01.11.2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах

персональных данных». При определении уровня защищённости ПДн, при их обработке в ИСПДн учитываются следующие исходные данные:

• категория обрабатываемых в информационной системе персональных данных;

• объём обрабатываемых персональных данных (количество субъектов персональных данных, персональные данные которых обрабатываются в информационной системе);

• заданные оператором характеристики безопасности персональных данных, обрабатываемых в информационной системе;

• тип угроз безопасности ПДн, актуальных для информационной системы;

• проверяется условие принадлежности ПДн сотрудникам оператора ПДн или иным субъектам, не являющимся сотрудниками оператора. По результатам анализа исходных данных информационных систем персональных данных присваивается соответствующий уровень защищённости ПДн, и составляется «Акт определения уровня защищённости ПДн, при их обработке в ИСПДн», утверждаемый руководителем Учреждения.

Уровень защищённости персональных данных может быть пересмотрен:

• по решению администратора информационной безопасности на основе проведённых им анализа и оценки угроз безопасности персональных данных с учётом особенностей и (или) изменений конкретной информационной системы;

• по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе.

9. ТРЕБОВАНИЯ К ПОДСИСТЕМАМ СЗПДн

Подсистемы СЗПДн имеют различную функциональность в зависимости от класса ИСПДн и уровня защищённости ПДн, определённого в Акте определения УЗ информационной системы персональных данных Учреждения.

В соответствии с руководящими документами регуляторов СЗПД может содержать до 10 подсистем, среди которых подсистема антивирусной защиты, защиты от утечки по техническим каналам, подсистема обеспечения безопасности межсетевого взаимодействия, анализа защищённости и выявления уязвимостей, криптографической защиты информации, подсистема обнаружения вторжений.

СЗПДн ОГБУ «КЦСО ЕАО» включает в себя следующие подсистемы:

- антивирусной защиты;
- управления доступом, регистрации и учёта;
- анализа защищённости.

9.1. Подсистема антивирусной защиты

Подсистема антивирусной защиты предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей ИСПДн Учреждения.

Средства антивирусной защиты предназначены для реализации следующих функций:

- резидентный антивирусный мониторинг;
- антивирусное сканирование;
- централизованная установка/деинсталляция антивирусного продукта, настройка, администрирование, просмотр отчётов и статистической информации по работе продукта;
- автоматизированное обновление антивирусных баз;
- автоматический запуск сразу после загрузки операционной системы.

Подсистема реализуется путём внедрения специального антивирусного программного обеспечения на все элементы ИСПДн.

9.2. Подсистема управления доступом, регистрации и учёта

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

- идентификации и проверки подлинности субъектов доступа при входе в ИСПДн;
- идентификации программ, томов, каталогов, файлов, записей, полей записей по именам;
- регистрации входа (выхода) субъектов доступа в систему (из системы), либо регистрации загрузки и инициализации операционной системы;
- 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 и СУБД).

9.3. Подсистема анализа защищённости

Подсистема анализа защищённости должна обеспечивать выявление уязвимостей, связанных с ошибками в конфигурации ПО ИСПДн.

Функциональность подсистемы может быть реализована программными и программно-аппаратными средствами.

10. МЕРЫ, МЕТОДЫ и СРЕДСТВА ОБЕСПЕЧЕНИЯ ТРЕБУЕМОГО УРОВНЯ ЗАЩИЩЁННОСТИ

Обеспечение требуемого уровня защищённости должно достигаться с использованием мер, методов и средств безопасности. Все меры обеспечения безопасности ИСПДн подразделяются на:

1) законодательные (правовые);
2) морально-этические;
3) организационные (административные);
4) физические;
5) технические (аппаратно-программные).

Перечень выбранных мер обеспечения безопасности отражается в Плане мероприятий по обеспечению защиты персональных данных в информационных системах персональных данных ОГБУ «КЦСО ЕАО».

10.1. Законодательные (правовые) меры обеспечения безопасности ИСПДн – действующие в Российской Федерации законы, указы и нормативные акты, регламентирующие правила обращения с ПДн, закрепляющие права и обязанности участников информационных отношений в процессе её обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию ПДн и являющиеся сдерживающим фактором для потенциальных нарушителей.

Законодательные (правовые) меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

10.2. Морально-этические меры обеспечения безопасности ИСПДн – нормы поведения, которые традиционно сложились или складываются по мере компьютеризации общества. Эти нормы большей частью не являются обязательными, как законодательно утверждённые нормативные акты, однако их несоблюдение ведёт обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний.

Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективе. Морально-этические меры защиты снижают вероятность возникновения негативных действий, связанных с человеческим фактором.

10.3. Административно-организационные меры обеспечения безопасности ИСПДн.

Реализация Политики информационной безопасности ПДн в ИСПДн состоит из мер административного уровня и организационных (процедурных) мер защиты информации.

Главная цель административных мер, предпринимаемых Учреждением – формирование основных подходов к защите информации и обеспечение их выполнения, с выделением необходимых ресурсов и контролем состояния дел.

К административному уровню относятся решения руководства Учреждения, затрагивающие деятельность ИСПДн в целом. Примером таких решений могут быть:

- формулирование целей, постановка задач, определение направлений деятельности в области безопасности ПДн;

- обеспечение нормативной (правовой) базы вопросов безопасности и т.п.

Организационные (процедурные) меры как составная часть СЗПДн включают в себя создание и поддержание в актуальном состоянии правовой базы безопасности ПДн, разработку и введение в действие организационно-распорядительных документов таких как:

- План мероприятий по обеспечению защиты персональных данных в информационных системах персональных данных ОГБУ «КЦСО ЕАО»;

- План внутренних проверок состояния системы защиты персональных данных в структурных подразделениях ОГБУ «КЦСО ЕАО»;

- Порядок резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации в информационных системах персональных данных ОГБУ «КЦСО ЕАО».

На организационном уровне определяются правила достижения целей и решения задач информационной безопасности ПДн. Эти правила определяют:

- какова область применения политики безопасности ПДн;

- каковы роли и обязанности должностных лиц, отвечающих за проведение политики безопасности ПДн, а так же их ответственность;

- кто имеет права доступа к ПДн;

- какими мерами и средствами обеспечивается защита ПДн;

- какими мерами и средствами обеспечивается контроль за соблюдением введённого режима безопасности.

Организационные меры предусматривают:

- регламент доступа в помещения ИСПДн;

- порядок допуска специалистов к использованию ресурсов ИСПДн;

- регламент процессов ведения баз данных и осуществления модификации информационных ресурсов;

- регламент процессов обслуживания и осуществления модификации аппаратных и программных ресурсов ИСПДн;

- инструкции пользователей ИСПДн (администратора безопасности ИСПДн, пользователя (оператора) ИСПДн);

- инструкции пользователя ИСПДн по обеспечению безопасности обработки персональных данных при возникновении нештатной ситуации.

10.4. Физические меры обеспечения безопасности ИСПДн – основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации. Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путём установления соответствующих постов охраны.

10.5. Технические (аппаратно-программные) меры обеспечения безопасности ИСПДн – основаны на использовании различных электронных устройств и специальных программ, входящих в состав ИСПДн и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты. Перечень необходимых мер и средств защиты информации определяется по результатам внутренней проверки обеспечения защиты ПДн в ИСПДн ОГБУ «КЦСО ЕАО».

В зависимости от определённого УЗ-4 ИСПДн и актуальных угроз, СЗПДн ОГБУ «КЦСО ЕАО» может включать следующие технические меры обеспечения безопасности ПДн:

- идентификация и аутентификация пользователей и объектов доступа;

- управление доступом пользователей к объектам доступа;

- антивирусные средства для АРМ пользователей и серверов;

- контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации;

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

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 Учреждения.

С учётом всех требований и принципов обеспечения безопасности ПДн в ИСПДн в состав системы защиты должны быть включены следующие средства защиты от несанкционированного доступа;

- средства идентификации (опознавания/логин) и аутентификации (подтверждения подлинности/пароль) пользователей ИСПДн;
- средства разграничения доступа зарегистрированных пользователей системы к ресурсам ИСПДн Учреждения;
- средства обеспечения и контроля целостности программных и информационных ресурсов.

Успешное применение технических мер обеспечения безопасности ИСПДн предполагает, что выполнение требований обеспечено организационными (административными) мерами и используемыми физическими средствами защиты:

- обеспечена физическая целостность всех компонентов ИСПДн;
- обеспечен учёт и хранение съёмных носителей информации и их обращение, исключающее хищение, подмену и уничтожение;
- обеспечено резервирование технических средств, дублирование носителей информации;
- обеспечено использование антивирусных средств защиты от вредоносного ПО и криптографических средств защиты информации;
- каждый пользователь ИСПДн или группа пользователей имеет уникальное системное имя и минимально необходимые для выполнения ими своих функциональных обязанностей полномочия по доступу к ресурсам системы;
- все изменения конфигурации технических и программных средств ИСПДн производятся в строго установленном порядке (регистрируются и контролируются) только на основании распоряжений руководства Учреждения;
- сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (специальных помещениях, шкафах и т.п.).
- специалистами Учреждения осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

11. ТРЕБОВАНИЯ К ПЕРСОНАЛУ ПО ОБЕСПЕЧЕНИЮ ЗАЩИТЫ ПДн

Работники Учреждения, являющиеся пользователями ИСПДн, должны чётко знать и строго выполнять установленные правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности ПДн.

При вступлении в должность нового работника непосредственный руководитель подразделения, 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.

Работники Учреждения, использующие технические средства аутентификации, должны обеспечивать сохранность идентификаторов (электронных ключей) и не допускать НСД к ним, а так же возможность их утери или использования третьими лицами. Пользователи несут персональную ответственность за сохранность идентификаторов.

Работники Учреждения должны следовать установленным процедурам поддержания режима безопасности ПДн при выборе и использовании паролей (если не используются технические средства аутентификации).

Работники Учреждения 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.

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

Работникам запрещается разглашать защищаемую информацию, которая стала им известна при работе с информационными системами Учреждения, третьим лицам.

При работе с ПДн в ИСПДн работники Учреждения обязаны обеспечить отсутствие возможности просмотра ПДн третьими лицами с мониторов АРМ.

Работники Учреждения должны быть проинформированы об угрозах нарушения режима безопасности ПДн и ответственности за его нарушение. Они должны быть ознакомлены с утверждённой формальной процедурой наложения дисциплинарных взысканий на сотрудников, которые нарушили принятые Политику и процедуры безопасности ПДн.

Работники обязаны без промедления сообщать обо всех наблюдаемых или подозрительных случаях работы ИСПДн, могущих повлечь за собой угрозы безопасности ПДн, а также о выявленных ими событиях, затрагивающих безопасность ПДн, руководству подразделения или администратору информационной безопасности.

12. ОТВЕТСТВЕННОСТЬ РАБОТНИКОВ УЧРЕЖДЕНИЯ

В соответствии со ст. 24 Федерального закона Российской Федерации от 27 июля 2006г. № 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 средств вычислительной техники, неправомерный доступ к информации, если эти действия привели к уничтожению, блокированию, модификации информации или нарушению работы средств вычислительной техники (статьи 272, 273 и 274 УК РФ).

Администратор информационной безопасности несёт ответственность за все действия, совершенные от имени его учётной записи или системных учётных записей, если не доказан факт несанкционированного использования учётных записей. При нарушениях пользователями ИСПДн правил, связанных с безопасностью ПДн, они несут ответственность, установленную действующим законодательством Российской Федерации.

13. КОНТРОЛЬ ЭФФЕКТИВНОСТИ СЗПДн

Целью контроля эффективности является своевременное выявление ненадлежащих режимов работы СЗПДн (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), а так же прогнозирование и превентивное реагирование на новые угрозы безопасности ПДн.

Контроль эффективности СЗПДн может проводиться как администратором безопасности ИСПДн (оперативный контроль в процессе информационного взаимодействия в ИСПДн), так и привлекаемыми для этой цели компетентными организациями, имеющими лицензию на этот вид деятельности.

Оценка эффективности СЗПДн проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

14. ОЖИДАЕМЫЙ ЭФФЕКТ ОТ РЕАЛИЗАЦИИ ПОЛИТИКИ

Реализация Политики информационной безопасности ПДн в ИСПДн ОГБУ «КЦСО ЕАО» позволяет:

1. оценивать состояние безопасности информации ИСПДн, своевременно выявлять источники внутренних и внешних угроз информационной безопасности, определять приоритетные направления предотвращения и нейтрализации этих угроз;
2. разрабатывать и поддерживать в актуальном состоянии организационно-распорядительные документы применительно к ИСПДн ОГБУ «КЦСО ЕАО»;
3. проводить организационные и технические мероприятия по обеспечению безопасности ПДн в ИСПДн Учреждения;
4. обеспечивать необходимый уровень безопасности объектов защиты.

Осуществление этих мероприятий обеспечивает создание единой и целостной системы информационной безопасности ИСПДн и создаёт условия для её дальнейшего совершенствования.

Приложение 1.

УРОВНИ ЗАЩИЩЁННОСТИ ИСПДн

(Согласно постановлению Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»)

Требования к защите ПДн / Уровень защищённости	**УЗ-1**	**УЗ-2**	**УЗ-3**	**УЗ-4**
Организация режима 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.	+	+	+	+
Утверждение руководителем оператора ПДн документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей.	+	+	+	+
Использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.	+	+	+	+
Необходимость назначения должностного лица (работника), ответственного за обеспечение безопасности персональных данных в информационной системе.	+	+	+	-
Возможность доступа к содержанию электронного журнала сообщений исключительно для должностных лиц (работников) оператора или уполномоченного лица, которым сведения, содержащиеся в указанном журнале, необходимы для выполнения служебных (трудовых) обязанностей.	+	+	-	-
Автоматическая регистрация в электронном журнале безопасности изменения полномочий сотрудника оператора по доступу к персональным данным, содержащимся в информационной системе.	+	-	-	-
Создание структурного подразделения, ответственного за обеспечение безопасности персональных данных в информационной системе, либо возложение на одно из структурных подразделений функций по обеспечению такой безопасности.	+	-	-	-

Приложение 2
к Составу и содержанию
организационных и технических мер по
обеспечению безопасности персональных
данных при их обработке в ИСПДн

Условное обозначение и номер меры	Содержание мер по обеспечению безопасности персональных данных	Уровни защищённости персональных данных			
		4	3	2	1
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)					
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	+	+	+
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных			+	+
ИАФ.3	Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов	+	+	+	+
ИАФ.4	Управление средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации	+	+	+	+
ИАФ.5	Защита обратной связи при вводе аутентификационной информации	+	+	+	+
ИАФ.6	Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей)	+	+	+	+
II. Управление доступом субъектов доступа к объектам доступа (УПД)					
УПД.1	Управление (заведение, активация, блокирование и уничтожение) учётными записями пользователей	+	+	+	+
УПД.2	Реализация необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа	+	+	+	+
УПД.3	Управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между информационными системами	+	+	+	+
УПД.4	Разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы	+	+	+	+
УПД.5	Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы	+	+	+	+
УПД.6	Ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе)	+	+	+	+
УПД.7	Предупреждение пользователя при его входе в информационную систему о том,				

	что в информационной системе реализованы меры по обеспечению безопасности персональных данных				
УПД.8	Оповещение пользователя после успешного входа в информационную систему о его предыдущем входе в информационную систему				
УПД.9	Ограничение числа параллельных сеансов доступа для каждой учётной записи пользователя информационной системы				
УПД.10	Блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу		+	+	+
УПД.11	Разрешение (запрет) действий пользователей, разрешённых до идентификации и аутентификации		+	+	+
УПД.12	Поддержка и сохранение атрибутов безопасности (меток безопасности), связанных с информацией в процессе её хранения и обработки				
УПД.13	Реализация защищённого удалённого доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети	+	+	+	+
УПД.14	Регламентация и контроль использования в информационной системе технологий беспроводного доступа	+	+	+	+
УПД.15	Регламентация и контроль использования в информационной системе мобильных технических средств	+	+	+	+
УПД.16	Управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы)	+	+	+	+
УПД.17	Обеспечение доверенной загрузки средств вычислительной техники			+	+
III. Ограничение программной среды (ОПС)					
ОПС.1	Управление запуском (обращениями) компонентов программного обеспечения, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов программного обеспечения				
ОПС.2	Управление установкой (инсталляцией) компонентов программного обеспечения, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов, контроль за установкой компонентов программного обеспечения			+	+
ОПС.3	Установка (инсталляция) только разрешённого к использованию программного обеспечения и (или) его компонентов				+
ОПС.4	Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов				
IV. Защита машинных носителей персональных данных (ЗНИ)					
ЗНИ.1	Учёт машинных носителей персональных данных			+	+
ЗНИ.2	Управление доступом к машинным носителям персональных данных			+	+
ЗНИ.3	Контроль перемещения машинных носителей персональных данных за пределы контролируемой зоны				
ЗНИ.4	Исключение возможности несанкционированного ознакомления с содержанием персональных данных, хранящихся на машинных носителях, и (или) использования носителей персональных данных в иных информационных системах				
ЗНИ.5	Контроль использования интерфейсов ввода (вывода) информации на машинные носители персональных данных				
ЗНИ.6	Контроль ввода (вывода) информации на машинные носители персональных данных				
ЗНИ.7	Контроль подключения машинных носителей персональных данных				
ЗНИ.8	Уничтожение (стирание) или обезличивание персональных данных на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) или обезличивания		+	+	+

V. Регистрация событий безопасности (РСБ)					
РСБ.1	Определение событий безопасности, подлежащих регистрации, и сроков их хранения	+	+	+	+
РСБ.2	Определение состава и содержания информации о событиях безопасности, подлежащих регистрации	+	+	+	+
РСБ.3	Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения	+	+	+	+
РСБ.4	Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объёма (ёмкости) памяти				
РСБ.5	Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них			+	+
РСБ.6	Генерирование временных меток и (или) синхронизация системного времени в информационной системе				
РСБ.7	Защита информации о событиях безопасности	+	+	+	+
VI. Антивирусная защита (АВЗ)					
АВЗ.1	Реализация антивирусной защиты	+	+	+	+
АВЗ.2	Обновление базы данных признаков вредоносных компьютерных программ (вирусов)	+	+	+	+
VII. Обнаружение вторжений (СОВ)					
СОВ.1	Обнаружение вторжений			+	+
СОВ.2	Обновление базы решающих правил			+	+
VIII. Контроль (анализ) защищённости персональных данных (АНЗ)					
АНЗ.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей		+	+	+
АНЗ.2	Контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации	+	+	+	+
АНЗ.3	Контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации		+	+	+
АНЗ.4	Контроль состава технических средств, программного обеспечения и средств защиты информации		+	+	+
АНЗ.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учётных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе			+	+
IX. Обеспечение целостности информационной системы и персональных данных (ОЦЛ)					
ОЦЛ.1	Контроль целостности программного обеспечения, включая программное обеспечение средств защиты информации			+	+
ОЦЛ.2	Контроль целостности персональных данных, содержащихся в базах данных информационной системы				
ОЦЛ.3	Обеспечение возможности восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций				
ОЦЛ.4	Обнаружение и реагирование на поступление в информационную систему незапрашиваемых электронных сообщений (писем, документов) и иной информации, не относящихся к функционированию информационной системы (защита от спама)			+	+
ОЦЛ.5	Контроль содержания информации, передаваемой из информационной системы (контейнерный, основанный на свойствах объекта доступа, и (или) контентный, основанный на поиске запрещённой к передаче информации с использованием сигнатур, масок и иных методов), и исключение неправомерной передачи информации из информационной системы				

ОЦЛ.6	Ограничение прав пользователей по вводу информации в информационную систему				
ОЦЛ.7	Контроль точности, полноты и правильности данных, вводимых в информационную систему				
ОЦЛ.8	Контроль ошибочных действий пользователей по вводу и (или) передаче персональных данных и предупреждение пользователей об ошибочных действиях				
X. Обеспечение доступности персональных данных (ОДТ)					
ОДТ.1	Использование отказоустойчивых технических средств				
ОДТ.2	Резервирование технических средств, программного обеспечения, каналов передачи информации, средств обеспечения функционирования информационной системы				
ОДТ.3	Контроль безотказного функционирования технических средств, обнаружение и локализация отказов функционирования, принятие мер по восстановлению отказавших средств и их тестирование				+
ОДТ.4	Периодическое резервное копирование персональных данных на резервные машинные носители персональных данных			+	+
ОДТ.5	Обеспечение возможности восстановления персональных данных с резервных машинных носителей персональных данных (резервных копий) в течение установленного временного интервала			+	+
XI. Защита среды виртуализации (ЗСВ)					
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	+	+	+	+
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	+	+	+	+
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре		+	+	+
ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры				
ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией				
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных			+	+
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций			+	+
ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры			+	+
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре		+	+	+
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки персональных данных отдельным пользователем и (или) группой пользователей		+	+	+
XII. Защита технических средств (ЗТС)					
ЗТС.1	Защита информации, обрабатываемой техническими средствами, от ее утечки по техническим каналам				
ЗТС.2	Организация контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования				
ЗТС.3	Контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения	+	+	+	+

	функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы, в помещения и сооружения, в которых они установлены				
ЗТС.4	Размещение устройств вывода (отображения) информации, исключающее её несанкционированный просмотр	+	+	+	+
ЗТС.5	Защита от внешних воздействий (воздействий окружающей среды, нестабильности электроснабжения, кондиционирования и иных внешних факторов)				
XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)					
ЗИС.1	Разделение в информационной системе функций по управлению (администрированию) информационной системой, управлению (администрированию) системой защиты персональных данных, функций по обработке персональных данных и иных функций информационной системы				+
ЗИС.2	Предотвращение задержки или прерывания выполнения процессов с высоким приоритетом со стороны процессов с низким приоритетом				
ЗИС.3	Обеспечение защиты персональных данных от раскрытия, модификации и навязывания (ввода ложной информации) при её передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи	+	+	+	+
ЗИС.4	Обеспечение доверенных канала, маршрута между администратором, пользователем и средствами защиты информации (функциями безопасности средств защиты информации)				
ЗИС.5	Запрет несанкционированной удалённый активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удалённо, и оповещение пользователей об активации таких устройств				
ЗИС.6	Передача и контроль целостности атрибутов безопасности (меток безопасности), связанных с персональными данными, при обмене ими с иными информационными системами				
ЗИС.7	Контроль санкционированного и исключение несанкционированного использования технологий мобильного кода, в том числе регистрация событий, связанных с использованием технологий мобильного кода, их анализ и реагирование на нарушения, связанные с использованием технологий мобильного кода				
ЗИС.8	Контроль санкционированного и исключение несанкционированного использования технологий передачи речи, в том числе регистрация событий, связанных с использованием технологий передачи речи, их анализ и реагирование на нарушения, связанные с использованием технологий передачи речи				
ЗИС.9	Контроль санкционированной и исключение несанкционированной передачи видеоинформации, в том числе регистрация событий, связанных с передачей видеоинформации, их анализ и реагирование на нарушения, связанные с передачей видеоинформации				
ЗИС.10	Подтверждение происхождения источника информации, получаемой в процессе определения сетевых адресов по сетевым именам или определения сетевых имён по сетевым адресам				
ЗИС.11	Обеспечение подлинности сетевых соединений (сеансов взаимодействия), в том числе для защиты от подмены сетевых устройств и сервисов			+	+
ЗИС.12	Исключение возможности отрицания пользователем факта отправки персональных данных другому пользователю				

ЗИС.13	Исключение возможности отрицания пользователем факта получения персональных данных от другого пользователя				
ЗИС.14	Использование устройств терминального доступа для обработки персональных данных				
ЗИС.15	Защита архивных файлов, параметров настройки средств защиты информации и программного обеспечения и иных данных, не подлежащих изменению в процессе обработки персональных данных			+	+
ЗИС.16	Выявление, анализ и блокирование в информационной системе скрытых каналов передачи информации в обход реализованных мер или внутри разрешённых сетевых протоколов				
ЗИС.17	Разбиение информационной системы на сегменты (сегментирование информационной системы) и обеспечение защиты периметров сегментов информационной системы			+	+
ЗИС.18	Обеспечение загрузки и исполнения программного обеспечения с машинных носителей персональных данных, доступных только для чтения, и контроль целостности данного программного обеспечения				
ЗИС.19	Изоляция процессов (выполнение программ) в выделенной области памяти				
ЗИС.20	Защита беспроводных соединений, применяемых в информационной системе		+	+	+
XIV. Выявление инцидентов и реагирование на них (ИНЦ)					
ИНЦ.1	Определение лиц, ответственных за выявление инцидентов и реагирование на них			+	+
ИНЦ.2	Обнаружение, идентификация и регистрация инцидентов			+	+
ИНЦ.3	Своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами			+	+
ИНЦ.4	Анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий			+	+
ИНЦ.5	Принятие мер по устранению последствий инцидентов			+	+
ИНЦ.6	Планирование и принятие мер по предотвращению повторного возникновения инцидентов			+	+
XV. Управление конфигурацией информационной системы и системы защиты персональных данных (УКФ)					
УКФ.1	Определение лиц, которым разрешены действия по внесению изменений в конфигурацию информационной системы и системы защиты персональных данных		+	+	+
УКФ.2	Управление изменениями конфигурации информационной системы и системы защиты персональных данных		+	+	+
УКФ.3	Анализ потенциального воздействия планируемых изменений в конфигурации информационной системы и системы защиты персональных данных на обеспечение защиты персональных данных и согласование изменений в конфигурации информационной системы с должностным лицом (работником), ответственным за обеспечение безопасности персональных данных		+	+	+
УКФ.4	Документирование информации (данных) об изменениях в конфигурации информационной системы и системы защиты персональных данных		+	+	+

Приложение 3.

РЕГИСТРАЦИЯ ИЗМЕНЕНИЯ ЛОКАЛЬНОГО НОРМАТИВНОГО ДОКУМЕНТА

Версия	**Наименование документа**	**Дата утверждения**
1	Политика информационной безопасности информационной системы персональных данных областного государственного бюджетного учреждения «Комплексный центр социального обслуживания Еврейской автономной области»	Приказ от 08.11.2017 № 302
2	Политика информационной безопасности информационных систем персональных данных областного государственного бюджетного учреждения «Комплексный центр социального обслуживания Еврейской автономной области»	Приказ от 12.04.2021 № 122